OCHRONA INTERESÓW FINANSOWYCH UNII EUROPEJSKIEJ – WSPÓLNE ZOBOWIĄZANIA I WYZWANIA

MATERIAŁY Z KONFERENCJI

SZKOŁA POLICJI KATOWICE

PROTEGERE ET PRODESSE IX

EUROPEAN ANTI-FRAUD OFFICE

Publikacja zawiera materiały z międzynarodowej konferencji pt.
Ochrona interesów finansowych Unii Europejskiej – wspólne zobowiązania i wyzwania,
która odbyła się w dniach 23-27 października 2017 r. w Katowicach,
zorganizowanej przez Szkołę Policji w Katowicach, Komendę Wojewódzką Policji w Opolu
i Komendę Wojewódzką Policji w Katowicach

This post-conference publication contains the texts of speeches delivered
at the international conference „Protection of the financial interests of the EU
– common obligations and challenges", which took place on 23-27 October 2017
in Katowice, organized by the Police School in Katowice, the Regional Police Headquarters
in Opole and the Regional Police Headquarters in Katowice

Projekt współfinansowany przez Program Unii Europejskiej Hercule III (2014-2020). Program jest
realizowany przez Komisję Europejską i został ustanowiony w celu promowania działalności
w dziedzinie ochrony interesów finansowych Unii Europejskiej (więcej informacji
na stronie: http://ec.europa.eu/anti_fraud/about-us/funding/index_en/htm

This conference is supported by the European Union Programme Hercule III (2014-2020).
This programme is implemented by the European Commission. It was established to promote activities
in the field of the protection of the financial interests of the European Union.

PROTEGERE ET PRODESSE IX

Ochrona interesów finansowych Unii Europejskiej – wspólne zobowiązania i wyzwania

Materiały z konferencji

Katowice 2017

Ochrona interesów finansowych Unii Europejskiej – wspólne zobowiązania i wyzwania
Materiały z konferencji

Część IX serii „Protegere et Prodesse" / Part IX of the series „Protegere et Prodesse"

Do publikacji dołączona jest płyta zawierająca prezentacje referatów wygłoszonych w czasie konferencji / The publication includes a DVD containing presentations delivered during the conference

Zespół redakcyjny / Editorial team:
Paweł Mięsiak
podinsp. Adam Warecki

Sekretarz redakcji / Editorial secretary:
Paulina Jamroga

Korekta, projekt graficzny, skład i przygotowanie do druku / Proofreading, composition and prepress:
Paweł Mięsiak

Druk / Print:
Drukarnia Kolumb, Chorzów

Wydawca / Editor: Szkoła Policji w Katowicach

ISBN 978-83-934380-6-8

Katowice, 2017 r.

SPIS TREŚCI • TABLE OF CONTENTS

insp. dr Rafał Kochańczyk

Przedmowa 9

Perface 11

Piotr Ryza

Kontrola projektów unijnych RPO WSL 2007-2013 13

Control of EU projects under the 2007-2013 Operational Programme for the Silesia Province (RPO WSL 2007-2013) 17

podinsp. Michał Pudło

Postępowanie przygotowawcze w sprawach dotyczących oszustw karuzelowych przy wykorzystaniu pracy operacyjnej – aspekty praktyczne 21

Preparatory proceedings with the use of operational work in cases regarding carousel fraud – practical aspects 29

Monika Duda-Szmyd

Błędy i nieprawidłowości w wydatkowaniu środków finansowych w projektach realizowanych w ramach RPO WSL 2007-2013 35

Errors and irregularities in spending financial funds in projects implemented as part of the 2007-2013 Regional Operational Programme for the Silesia Province (RPO WSL 2007-2013) 37

mł. insp. Piotr Trzciński

Konfiskata rozszerzona oraz nowe uprawnienia polskich organów ścigania w zwalczaniu przestępczości zorganizowanej zmierzające do ujawnienia i konfiskaty nielegalnych dochodów 39

Extended Confiscation and new rights of Polish law enforcement agencies in combating organised crime aimed at identifying and confiscating of unlawful profits 47

Betina Tynka, Tomasz Zaborowski
Informatyka śledcza w zwalczaniu przestępstw korupcyjnych i gospodarczych 55
Computer forensics in combating corruption and economic crime 59

Krzysztof Mendyk
Transfery pieniężne z krajów UE do krajów Dalekiego Wschodu niemające odzwierciedlenia w transakcjach gospodarczych 63
Money transfers from EU countries to Far Eastern countries that are not reflected in economic transactions 67

Jacek Baranowski
The role, and support of EUROPOL in financial investigations. Cooperation with Member States 71
Rola i wsparcie Europolu w dochodzeniach finansowych. Współpraca z państwami członkowskimi Unii Europejskiej 79

podkom. SC Kamilla Siwek
Zagrożenia w obrocie krajowym i międzynarodowym wyrobami energetycznymi 87
Threats in trading of energy products (domestic and international trade) 93

podinsp. Michał Pudło
Ujawnianie i zabezpieczenie mienia – praca operacyjna jako wsparcie postępowania procesowego 97
Disclosure of and seizure of property – operational work as support of procedural acts 101

Arkadiusz Pytlik
Analiza kryminalna w służbach bezpieczeństwa wewnętrznego 105
Criminal analysis in internal security services 157

Andrew Tennant
Crypto Currency (Bitcoin) – guide for search officers 207
Kryptowaluta (bitcoin) – informacje dla funkcjonariuszy prowadzących przeszukania 213

Brian Ludlow
Trade Based Money Laundering (TMBL) 219
Pranie brudnych pieniędzy w obrocie handlowym (TBML) 231

Ian Pemberton
Financial investigation methods by the Irish Police Force and the international cooperation to fight financial fraud 245
Metody prowadzenia dochodzeń finansowych przez policję Irlandii i międzynarodowa współpraca w walce z oszustwami finansowymi 255

Giles Orton
Training Methods for Officers Combating Crime in the UK 267
Metody szkoleniowe funkcjonariuszy zwalczających przestępczość w Wielkiej Brytanii 279

Przedmowa

Publikacja, którą oddajemy w Państwa ręce zawiera materiały z międzynarodowej konferencji „Ochrona interesów finansowych Unii Europejskiej – wspólne zobowiązania i wyzwania", która odbyła się w dniach 23-27 października 2017 r.

Współczesne metody działalności przestępczej od dawna nie uznają granic. Wraz ze zwiększeniem się liczby zadań Wspólnoty Europejskiej oraz wzrostem środków finansowych przeznaczonych na ich realizację, wzrasta potrzeba ochrony budżetu ogólnego i innych instrumentów systemu finansowego UE przed przestępczymi procederami.

Można powiedzieć, że organy prawa zawsze będą o pół kroku za przestępcami. Wynika to z różnych okoliczności, na przykład regulacji prawnych, struktur do walki z tymi patologiami itp. Nie oznacza to jednak, że biernie się przyglądamy. Wręcz przeciwnie, gdy spojrzymy na tematy wystąpień naszych prelegentów możemy zauważyć, że ta konferencja była miejscem, w którym doszło do wymiany informacji na temat zagrożeń, skutecznych metod zapobiegania i ścigania sprawców tego typu przestępstw. Cieszę, że w tym spotkaniu wzięło udział tak wielu przedstawicieli reprezentujących różne podmioty, które na co dzień zajmują się zwalczaniem tego rodzaju procederu.

Chciałbym w tym miejscu podziękować wszystkim tym, których ciężka praca zaowocowała realizacją konferencji. Szczególne słowa uznania kieruję pod adresem podinsp. Adama Wareckiego.

Bardzo dziękuję wszystkim prelegentom, którzy wystąpili w ciągu tych 5 dni. Tematyka wystąpień wyraźnie wskazuje, że mamy do czynienia z profesjonalistami, z wiedzy których warto korzystać.

Mam nadzieję, że konferencja „Ochrona interesów finansowych UE – wspólne zobowiązania i wyzwania" spełniła oczekiwania i długo pozostanie w pamięci uczestników, nie tylko z powodu wysokiego poziomu obrad, ale również ze względu na jej rolę integracyjną.

insp. dr Rafał Kochańczyk
Komendant Szkoły Policji w Katowicach

Perface

It is my great pleasure to present this publication related to the international conference „Protection of the financial interests of the EU – common obligations and challenges", which took place on 23-27 October 2017.

Modern day methods of criminal activity have long ceased to recognise borders. The growing number of tasks faced by the European Community and the increasing volume of funds allocated to implement these tasks have been followed by a greater need to protect the general budget and other instruments of the EU financial system against criminal practices.

It can be said that law enforcement agencies will always be half a step behind criminals. This is a result of various circumstances e.g. legal regulations, the structure for combating those pathologies etc. It does not mean, however, that we sit idly watching. Just the opposite, when you take a look at the subjects raised by our speakers you will notice that this conference was a forum for exchanging information on the threats, effective methods of prevention and prosecution of perpetrators of these crimes. I am happy to have seen so many representatives of various entities that deal with combating this type of crime on a day-to-day basis.

On this occasion, I would like to thank all those people whose hard work has made this conference come true. My words of special recognition go to Major Adam Warecki.

I would like to thank all speakers who presented their papers during the conference. The subject range of the papers clearly shows that we are dealing with experts whose knowledge is a valuable thing to share.

I hope that the conference „Protection of the financial interests of the EU – common obligations and challenges" met your expectations, was a satisfying experience and will long remain in the memory of the participants, not only because of the high quality of its content, but also because of its integration and bonding value.

col. dr Rafał Kochańczyk
Commandant of The Police School in Katowice

Piotr Ryza
Wydział Europejskiego Funduszu Rozwoju Regionalnego – Urząd Marszałkowski Województwa Śląskiego

Kontrola projektów unijnych RPO WSL 2007-2013

Streszczenie

Prezentacja pt.: „Kontrola projektów unijnych RPO WSL 2007-2013" – jej głównym przesłaniem będzie próba zaprezentowania potrzeby współpracy organów ścigania z urzędami (Instytucjami Zarządzającymi) w kontekście szczególnego pożądania/zainteresowania osób nieuczciwych w zakresie pozyskiwania i wydatkowania środków unijnych. Jednocześnie chciałbym udowodnić, że nie istnieje (nie jest możliwe) skuteczne zarządzanie środkami bez funkcjonowania odpowiedniego systemu kontroli. W pierwszej kolejności przybliżę organizację referatu kontroli, zadania oraz krótką statystykę. Omówione zostaną rodzaje, procedury oraz zakres kontroli. Przedstawione zostaną typy nieprawidłowości, metody ich wykrycia oraz na wybranych projektach realizowanych w ramach RPO WSL 2007-2014 przykłady nieprawidłowości. Dodatkowo przybliżę współpracę IZ RPO WSL z Policją oraz innymi organami ścigania.

Efektywne zarządzanie środkami pochodzącymi zarówno z funduszy strukturalnych, jak i Funduszu Spójności nie jest możliwe bez funkcjonowania odpowiedniego systemu kontroli.

Powyższa sentencja została określona w motywie 66 preambuły Rozporządzenia Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r. ustanawiającego przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności i uchylające rozporządzenie (WE) nr 1260/1999.

Mając na uwadze powyższe Instytucja Zarządzająca Regionalnym Programem Operacyjnym Województwa Śląskiego 2007-2013 zwana dalej „IZ RPO WSL 2007-2013" powierzyła realizację zadań w zakresie kontroli projektów referatowi kontroli projektów zwanemu dalej „RKPR" składającemu się z 24 osób, który został podzielony na dwa zespoły: zespół ds. kontroli projektów (15 osób) oraz zespół ds. kontroli zamówień (6 osób). Dodatkowo w skład RKPR wchodziło stanowisko pomocy administracyjnej i samodzielne stanowisko ds. kontroli zewnętrznych.

Kontrole projektów realizowano, uwzględniając następujące formy przeprowadzania kontroli, a mianowicie kontrole: na zakończenie realizacji projektu, w trakcie realizacji projektu, doraźne, sprawdzające trwałość projektu oraz krzyżowe.

Mając na celu sprawne wdrażanie RPO WSL przyspieszony został proces rozliczania projektów oraz skrócono czas oczekiwania na kontrolę przy jednoczesnym zapewnieniu jej odpowiedniej jakości, poprzez wprowadzenie mechanizmu doboru próby do kontroli na miejscu.

W celu wytypowania projektów do kontroli na miejscu realizacji (za pomocą doboru próby) przeprowadzano analizę ryzyka, a dobór próby do kontroli na miejscu opierał się na analizie następujących czynników (kryteriów) zawartych w matrycy ryzyka:

- wartość projektu,
- rodzaj beneficjenta,
- liczba realizowanych przez beneficjenta projektów współfinansowanych przez UE w ramach RPO WSL,
- zamówienia publiczne,
- liczba postępowań o udzielenie zamówienia publicznego w ramach danego/badanego projektu,
- partnerzy w projekcie,
- powiązanie z PROW,
- projekt generujący dochód (w myśl art. 55 Rozporządzenia Rady (WE) nr 1083/2006 z dnia 11 lipca 2006 r.).

W wyniku przeprowadzonej analizy ryzyka, na podstawie określonego stopnia ryzyka (0 ÷ 100 %), każdy z projektów przyporządkowany został do jednej z dwóch grup ryzyka:

- projekty podwyższonego ryzyka – gdy stopień ryzyka był równy lub wyższy niż 60%,
- projekty niskiego ryzyka – gdy stopień ryzyka był niższy niż 60%.

W przypadku projektów o podwyższonym ryzyku nie stosowano metody doboru próby, gdyż kontrolą na miejscu objęto w tej grupie wszystkie projekty. Dodatkowo IZ RPO WSL 2007-2013 mogła wybrać do kontroli na miejscu realizacji projekty z grupy projektów o niskim ryzyku. W takim przypadku do kontroli stosowano dobór celowy (dobór ekspercki) polegający na profesjonalnym osądzie audytorskim (kontrolnym). Nadmienić należy, iż przy doborze projektów do kontroli nie rządził przypadek, lecz ściśle określona kalkulacja merytoryczna prowadzącego dobór.

Jednocześnie określone zostały obowiązkowe kontrole na miejscu realizacji, które były wyłączone z doboru próby:

- projekty dla których beneficjentem było województwo śląskie,
- projekty realizowane w ramach Priorytetu 10 (Roczne Plany Działań),
- projekty o wartości powyżej 20 mln złotych (koszt całkowity).

Podkreślenia wymaga fakt, iż w przypadku kontroli na zakończenie realizacji projektu (tj. po wpłynięciu wniosku o płatność końcową) bezwzględnie muszą zostać sprawdzone w sposób możliwie szczegółowy m.in. wszystkie dokumenty i wydatki poniesione w ramach projektu oraz skontrolowane fizyczne efekty realizowanego projektu, w taki sposób, aby można było uzyskać uzasadnioną pewność, że projekt został zrealizowany poprawnie, a zakładane rezultaty i cel projektu osiągnięte.

Kontrola projektu na miejscu obejmuje następujące podstawowe etapy:

1. zaplanowanie czynności kontrolnych i sporządzenie upoważnień do kontroli;
2. przekazanie beneficjentowi zawiadomienia o kontroli;
3. przeprowadzenie czynności kontrolnych;
4. sporządzenie i przekazanie informacji pokontrolnej jednostce kontrolowanej;
5. sporządzenie i przekazanie zaleceń pokontrolnych jednostce kontrolowanej (jeśli dotyczy);

6. weryfikacja wykonania zaleceń pokontrolnych lub przeprowadzenie kontroli sprawdzającej (jeśli dotyczy);
7. dokumentowanie czynności kontrolnych, raportowanie oraz wprowadzenie informacji o przeprowadzonych kontrolach do systemów informatycznych (LSI, KSI).

W opisywanym okresie programowania IZ RPO WSL 2007-2013 podpisała 1809 umów o dofinansowanie (bez projektów dofinansowanych w ramach działań realizowanych przez Śląskie Centrum Przedsiębiorczości), z czego zrealizowano 1772 projektów, a 37 umów o dofinansowanie rozwiązano.

Referat RKPR przeprowadził 2783 kontrole w ramach RPO WSL 2007-2013 (bez kontroli trwałości). 911 kontroli zakończyło się istotnymi zastrzeżeniami mającymi skutki finansowe[1].

W całym okresie programowania IZ RPO WSL 2007-2013 wielokrotnie współpracowała z organami ścigania, a największy udział w tym zakresie przypadł referatowi RKPR. Zgodnie bowiem z ustawą z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (tekst jednolity Dz.U. z 2017 r. poz. 1904) zwanym dalej k.p.k. wszystkie instytucje państwowe, samorządowe i społeczne mają obowiązek współpracy i udzielania pomocy organom ścigania (art. 15 § 2 oraz 304 § 2 k.p.k.). Zasadnym jest wskazać, iż współpraca z organami ścigania ma wymiar szczególny, gdyż nie stanowi ona tylko i wyłącznie wykonania obowiązku określonego w przepisach, lecz należy ją postrzegać w szerszym aspekcie. Należy uzmysłowić sobie, że środki unijne są bardzo zagrożone w kontekście szczególnego pożądania i zainteresowania osób nieuczciwych zarówno w zakresie ich pozyskiwania, jak i wydatkowania. Z tego też powodu instytucje powołane do wdrażania środków unijnych w Polsce winny być zobowiązane do wspierania oraz ścisłej współpracy, a nawet współistnienia z Policją oraz innymi organami ścigania w zakresie ujawniania i zwalczania przestępczości na szkodę Unii Europejskiej. W ramach obopólnych korzyści Policja, jak również inne służby powinny współpracować z podmiotami posiadającymi uprawnienia kontrolne w ramach środków pochodzących z budżetu UE.

[1] Na podstawie danych z LSI SIWIZ.

Piotr Ryza

Department of the European Regional Development Fund Marshal Office Silesian Voivodeship

Control of EU projects under the 2007-2013 Operational Programme for the Silesia Province (RPO WSL 2007-2013)

Abstract

„Control of EU projects under the 2007-2013 Operational Programme for the Silesia Province (RPO WSL 2007-2013)" – the main message of this presentation will be to demonstrate the need for cooperation between law enforcement agencies and authorities (Managing Authorities) in the context of a special interest of unfair individuals in acquiring and spending Community funds. I would also like to demonstrate that funds cannot be managed effectively without an appropriate system of control. First off all, I will discuss the structure and tasks of the control office as well as brief statistics. Then I will proceed to discussing types, procedures and scope of controls. I will present types of irregularities and methods of detection, as well as some examples of irregularities - based on selected projects implemented under RPO WSL 2007-2014. Apart from that, I will briefly review cooperation between the Managing Authority IZ RPO WSL with the Police and other law enforcement agencies.

Effective management of resources both from structural funds and the Cohesion Fund is not be possible without an appropriate system of control in place.

This sentence is set out in recital 66 of the preamble to Council Regulation (EC) No. 1083/2006 of 11 July 2006 laying down general provisions on the European Regional Development Fund, the European Social Fund and the Cohesion Fund and repealing Regulation (EC) No. 1260/1999.

Having regard to the above, the Authority Managing the 2007-2013 Regional Operational Programme for the Silesia Province, hereinafter referred to as „the IZ RPO WSL 2007-2013", entrusted the implementation of the project control tasks to the Project Control Section, hereinafter referred to as the „RKPR", made up of 24 persons divided into two teams: the Project Control Team (15 persons) and the Contract Control Team (6 persons). In addition, the RKPR's structure included the Administrative Support function and the independent function for External Audits.

The project control was conducted by means of the following control methods: controls at the project completion, controls during the project implementation, ad hoc controls, project sustainability controls and cross checks.

In order to ensure efficient implementation of the RPO WSL, the project settlement process was accelerated and the control waiting time was reduced while ensuring appropriate

quality of the controls by introducing the mechanism of selecting samples on site. In order to select projects to be controlled on site (by means of sample selection), a risk analysis was conducted and the selection of samples to be controlled on site was based on an analysis of the following factors (criteria) identified in the Risk Matrix:

- value of the project;
- category of the beneficiary;
- number of the beneficiary's projects financed by the EU under the RPO WSL;
- public procurement;
- number of public contract award procedures in a given/examined project;
- partners in the project;
- links to the RDP;
- revenue-generating projects (in accordance with Article 55 of Council Regulation (EC) No. 1083/2006 of 11 July 2006).

Based on the risk level (0 ÷ 100 %) identified in the course of the risk analysis, each project was allocated to either of the two following risk groups:

- higher-risk projects – if the risk level was equal to or higher than 60%;
- low-risk projects – if the risk level was lower than 60%.

The sample selection method was not employed for the higher-risk projects, for all projects in this group were subjected to on-site controls. In addition, the IZ RPO WSL 2007-2013 was allowed to select also some projects of the low-risk group to be controlled on site. In such cases, controls were conducted on the basis of a targeted selection (expert selection) which consisted in a professional auditor (control) assessment. It must be noted that the selection of projects to be controlled was not random, but based on a precise substance-based calculation by the selecting person.

At the same time, compulsory on-site controls were planned for cases excluded from the sample selection method:

- projects where the Silesia Province was the Beneficiary;
- projects implemented as part of Priority 10 (Annual Action Plans);
- projects worth more than PLN 20 million (total cost).

It must be emphasised that project-end controls (i.e. ones conducted after submission of the final payment application) must verify, in the most detailed extent possible, all documents and expenditures incurred as part of the project and check the physical effects of the project so that it can be established with a reasonable degree of certainty that the project has been implemented appropriately and the assumed outcomes, and the objective of the project have been achieved.

On-site project controls include the following basic stages:

- planning of the control actions and preparing authorisations to control;
- providing the beneficiary with a notice of control;
- conducting the control actions;
- preparing and submitting post-control information to the controlled unit;
- preparing and submitting post-control recommendations to the controlled unit (if applicable);

- verifying implementation of the post-control recommendations or performing a follow--up control (if applicable);
- documenting the control actions, reporting and entering information on the completed controls into IT systems (LSI, KSI).

In the programme period in question, the IZ RPO WSL 2007-2013 signed 1,809 funding contracts (excluding projects financed as part of actions implemented by the Silesian Centre for Entrepreneurship), of which 1772 projects were completed and 37 funding contract were terminated.

The RKPR conducted 2783 controls under the RPO WSL 2007-2013 (excluding sustainability controls). 911 controls brought material reservations leading to financial consequences[1].

Throughout the programme period in question, the IZ RPO WSL 2007-2013 cooperated with law enforcement agencies on numerous occasions, with the bulk of the cooperation carried out by the RKPR. In accordance with the Code of Criminal Procedure of 6 June 1997 (official codification: Journal of Laws 2017, Item 1904), hereinafter referred to as the CCP, all state, local government and social authorities are obliged to cooperate with and provide assistance to law enforcement agencies (Article 15 Section 2 and Article 304 Section 2 of the CCP). It is appropriate to note that such cooperation with law enforcement agencies is unique, as it is not only the fulfilment of the obligation prescribed by law, but should be considered in a broader context. One must be aware that EU funds are very vulnerable in because they are a subject of particular desire and interest of dishonest individuals in terms of their acquisition and spending. This is why authorities in charge of implementing the EU funds in Poland should be obliged to support and closely cooperate with, and even coexist, with the Police and other law enforcement agencies in the area of disclosing and combating crime against the European Union. In turn, in view of mutual benefits, the Police and other services should cooperate with entities authorised to control implementation of funds from the EU budget.

[1] According to the local computer system LSI SIWIZ.

podinsp. Michał Pudło
Wydział Wywiadu Kryminalnego Zarządu CBŚP w Katowicach

Postępowanie przygotowawcze w sprawach dotyczących oszustw karuzelowych przy wykorzystaniu pracy operacyjnej – aspekty praktyczne

Streszczenie

Rosnąca luka podatkowa w podatku VAT, której główną przyczyną są wyłudzenia podatkowe, przybrała rozmiary i strukturę godzące w bezpieczeństwo ekonomiczne Państwa. W konsekwencji mogą prowadzić do wyparcia z rynku uczciwych przedsiębiorców, którzy nie są w stanie sprostać konkurencji „dotowanej" przez przejęte wskutek działań przestępczych podatki.
Tzw. „oszustwa karuzelowe" są najpoważniejszymi przestępstwami skarbowymi w całej Unii Europejskiej. Aby cały mechanizm się opłacał podmioty lub podmiot w tzw. „łańcuchu transakcji" nie wpłacając należnego VAT-u, a inny nienależnie wystąpić o jego zwrot.
Zwalczanie tego typu przestępczości zorganizowanej wymaga pełnej współpracy pomiędzy służbami w których właściwości przedmiotowej jest zajmowanie się przestępstwami karno-skarbowymi oraz zwalczenie zorganizowanej przestępczości. Skomplikowane prowadzenie czynności o charakterze procesowym musi przebiegać równolegle przy pełnej transparentności z prowadzeniem czynności o charakterze operacyjnym. Tylko przenikanie się zakresów i uprawnień tych dwóch rodzajów czynności pozwala na osiągnięcie sukcesów w zwalczaniu tego rodzaju przestępczości.

Rosnąca luka podatkowa w podatku VAT, której główną przyczyną są wyłudzenia podatkowe, przybrała rozmiary i strukturę godzące w bezpieczeństwo ekonomiczne Państwa. Uszczuplenia podatkowe uderzają również w bezpieczeństwo obrotu gospodarczego poprzez naruszenie zasad uczciwej konkurencji. W konsekwencji mogą prowadzić do wyparcia z rynku uczciwych przedsiębiorców, którzy nie są w stanie sprostać konkurencji „dotowanej" przez przejęte wskutek działań przestępczych podatki.

Tzw. „oszustwa karuzelowe" są najpoważniejszymi przestępstwami skarbowymi w całej Unii Europejskiej. Aby cały mechanizm się opłacał podmioty lub podmiot w tzw. „łańcuchu transakcji" nie wpłacając należnego VAT-u, a inny nienależnie wystąpuje o jego zwrot. W związku z tym częścią procederu muszą być tzw. „znikający podatnicy – słupy", osoby wystawiające faktury, które nie mają odzwierciedlenia w realnych transakcjach, nie płacące podatków od wystawionych dokumentów. „Karuzelowe oszustwa" to w praktyce zorganizowana, hierarchicznie zbudowana przestępczość na olbrzymią skalę, zagrażająca podstawom

finansów publicznych. Celem procederu jest najczęściej wyłudzenie podatku VAT, który w rzeczywistości nigdy wcześniej nie został zapłacony, ale także uniknięcie opodatkowania. Celem „karuzeli" może być także wprowadzenie do obrotu towarów z nielegalnych źródeł, np. z przemytu lub zalegalizowanie środków finansowych, czyli pranie pieniędzy. Taki proceder pozwala również na obniżenie cen towarów, by zaoferować na rynku krajowym warunki konkurencyjne w stosunku do przedsiębiorców, sprzedających te same produkty, ale funkcjonujących legalnie.

Obecnie w Polsce prowadzonych jest około 100 śledztw (najpoważniejszych, w których wartość uszczupleń lub nienależnego zwrotu podatku VAT przewyższa kwotę 1 mln złotych), a łączna kwota uszczuplonych należności publicznoprawnych, stwierdzonych w tych postępowaniach przygotowawczych, to kwota 5 miliardów złotych. Podkreślić należy, że większość postępowań dotyczy przestępczej działalności w latach wcześniejszych, tj. od 2010 do 2014 r.

Zwalczanie tego typu przestępczości zorganizowanej wymaga pełnej współpracy pomiędzy służbami, w których właściwości przedmiotowej jest zajmowanie się przestępstwami karno-skarbowymi oraz zwalczenie zorganizowanej przestępczości.

Wyrażenie „karuzela podatkowa" odnosi się do sposobu, w jaki sprzedawane towary krążą między poszczególnymi podmiotami zaangażowanymi w oszustwo. Towary są różne – od paliw do złota. Przeważają drogie jednostkowo przedmioty, o niewielkich rozmiarach, ale cieszące się popularnością na rynku, gdyż są łatwo zbywalne. Umożliwia to wygenerowanie w krótkim czasie znacznej skali obrotu, by szybko uzyskać wysoki zwrot podatku VAT. Wykorzystywane są towary, które stosunkowo łatwo można przemieszczać pomiędzy firmami. Z praktyki wynika, że największe wyłudzenia odbywają się w handlu paliwem, złomem, telefonami komórkowymi, sprzętem elektronicznym i komputerowym, aplikacjami na smartfony czy tablety.

Grupy przestępcze działają w ten sposób, że w momencie, kiedy stwarzamy im niekorzystne warunki do działania w jednej branży, przenoszą się natychmiast do drugiej. Przykładem była branża handlu złomem. Po zastosowaniu metody odwróconego obciążenia podatkiem VAT przestępcy przenieśli się na innego rodzaju produkty, m.in. stal.

Państwo nie jest w stanie nadążyć ze zmianami przepisów w ten sposób, żeby wyeliminować oszustwa w całym spektrum danej branży. Im większa wartość danego towaru, tym większy podatek VAT do zwrotu.

Podmioty występujące w karuzelach podatkowych

„Słup" lub znikający podatnik to podmiot użyty do stworzenia pozorów rzeczywistego funkcjonowania w transakcjach wewnątrzwspólnotowych, w których głównym celem jest uzyskanie oszukańczego zysku z VAT, nałożonego na następną transakcję.

Cechy charakterystyczne:

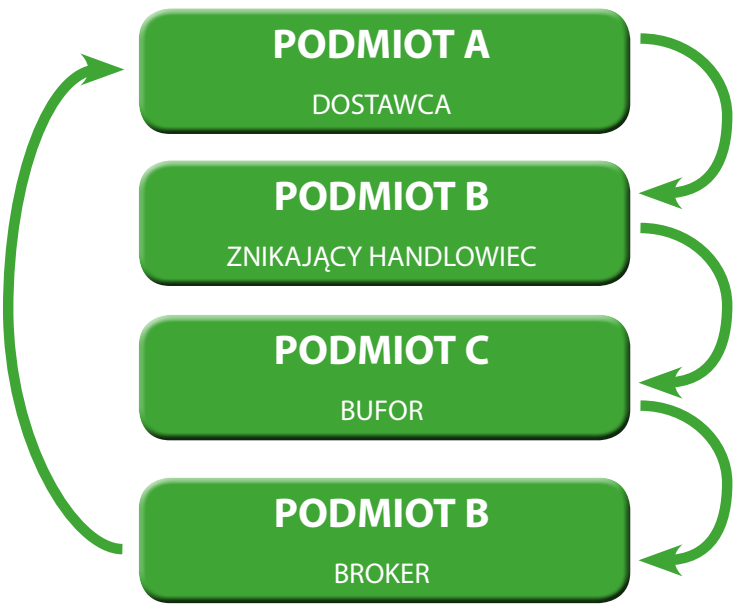
- nie wywiązuje się z zobowiązań podatkowych – nie płaci podatku oraz nie składa deklaracji podatkowych. Jeśli składa deklaracje, to tzw. „deklaracje zerowe",
- działa krótko (od kilku do kilkunastu miesięcy),
- nie prowadzi rzeczywistej działalności (podaje adres mieszkania lub adres jest sfałszowany),

- nie posiada ani aktywów ani środków do prowadzenia działalności,
- dokonuje WNT (wewnątrzwspólnotowych nabyć towarów) i dostawy krajowej na rzecz przedsiębiorstwa buforowego lub brokera,
- dla zmylenia organów podatkowych może oprócz dostawy krajowej dokonywać dostaw wewnątrzwspólnotowych,
- często jest to sp. z o.o. – członkowie zarządu są podstawieni lub ich firmy zagraniczne są zarejestrowane w tzw. „rajach podatkowych" (administracja podatkowa nie ma dostępu do ich dokumentów).

„Broker", nazywany również „wykładowcą VAT-u", „sponsorem VAT", „operatorem" – firma, która jest końcowym ogniwem i jednym z odbiorców zysku z oszukańczego planu, usytuowany w tym samym kraju członkowskim UE co znikający podatnik, nabywa towary i/lub usługi od bufora i dostarcza je do podmiotu zagranicznego na zasadzie WDT (wewnątrzwspólnotowych dostaw towaru), Podmiot nabywający od bufora (rzadziej od znikającego podatnika) i dokonujący WDT do spółki wiodącej lub dostawy krajowej na rynek krajowy.

Cechy charakterystyczne:

- składa wniosek o zwrot podatku VAT od dokonanych zakupów lub wpłaca niewielką nadwyżkę podatku należnego nad naliczonym,
- broker może działać jako bufor, np. dokonywać transakcji związanych z oszustwem do innych podmiotów w tym samym kraju członkowskim,
- czasami jest tzw. „podmiotem wiodącym" czyli najpoważniejszym podmiotem i organizatorem w oszustwach karuzelowych, stwarza pozory przestrzegania przepisów prawa i działania w dobrej wierze, posiada kapitał i zaplecze, umożliwiające wiarygodne powadzenie działalności gospodarczej,



Schemat działania karuzeli podatkowej

- prawidłowo prowadzi księgowość, składa deklaracje podatkowe i reguluje terminowo zobowiązania publicznoprawne (zazwyczaj jednak w niewielkich kwotach),
- jest podmiotem zarejestrowanym w tym samym państwie członkowskim na terytorium którego funkcjonuje znikający podatnik.

Podmiot zagraniczny – podmiot najczęściej czeski lub słowacki wykorzystywany jest do tzw. „zerowania VAT-u". Pozornie towar i faktury sprzedaży od podmiotów polskich – firm zwanych operatorami, beneficjentami VAT-u lub wykładowcami VAT-u, (ze stawką 0% podatku VAT z uwagi na wewnątrzwspólnotowe dostawy towarów) są sprzedawane do tego podmiotu, a następnie pozornie towar wraca do Polski fakturowo do kolejnych ogniw „karuzeli vatowskiej" (ze stawką 0% podatku VAT) tzw. firm „słupów" – znikających podatników, skąd następnie jest przekazywany (ze stawką 23% podatku VAT) do firm tzw. „buforów". Często jako właściciele lub członkowie zarządów pomiotów czeskich lub słowackich są obywatele polscy.

Gromadzenie dowodów – pierwsze czynności procesowe

Dla zapewnienia prawidłowego toku czynności śledczych koniecznym jest systematyczne gromadzenie informacji o podmiotach gospodarczych uczestniczących w procederze, w tym dane z:

- administracji skarbowej,
- ZUS,
- Krajowego Rejestru Sądowego lub ewidencji działalności gospodarczej,
- rachunków bankowych,
- danych telekomunikacyjnych,
- innych (koncesje, zezwolenia itp.)

Konieczne jest także od samego rozpoczęcia czynności systematyczne gromadzenie informacji o osobach (PESEL, CBA, rachunki bankowe). Zgromadzone dane i informacje należy gromadzić w sposób umożliwiający ich szybkie zlokalizowanie i natychmiastowe wykorzystanie. Pomocne w tej materii są narzędzia analityczne, nie tylko profesjonalne jak do analizy kryminalnej ale najprostsze arkusze kalkulacyjne.

Zabezpieczenie dokumentacji finansowo-księgowej

Dokumentacja musi obejmować przepływ towarów (np. CMR, dokumenty magazynowe, transportowe), dokumentację handlową (faktury, umowy), przepływ środków finansowych (dokumentacja bankowa, kasowa). Zabezpieczeniu powinny podlegać również, a może przede wszystkim, wersje elektroniczne takiej dokumentacji. Ułatwi to i przyśpieszy znacznie dalsze prowadzenie czynności, w tym analitycznych.

Najczęstsze błędy w zabezpieczeniu dokumentów:

- zabezpiecza się tylko faktury, bez dokumentacji transportowej, bez dokumentacji płatności,
- zabezpiecza się dokumenty transportowe (CMR), bez ich analizy i dalszych sprawdzeń u przewoźników,

- nie dokonuje się zabezpieczenia dalszej dokumentacji bankowej ponad przekazaną przez GIIF, często ma ona szczątkowy charakter, nie występuje się o historię rachunków bankowych, która wynika z analizy nowej zabezpieczonej w sprawie dokumentacji,
- brak zabezpieczenia wersji elektronicznej dokumentacji.

Najważniejsze dokumenty do zabezpieczenia:

- faktury,
- CMR-y,
- rejestr sprzedaży i zakupu VAT,
- deklaracja,
- dokumenty magazynowe,
- rachunki bankowe,
- dokumenty typu KP lub DW i inna dokumentacja kasowa,
- karty płatnicze,
- akty notarialne,
- notatki, schematy.

Jakie miejsca warto przeszukać:

- miejsca prowadzenia działalności,
- miejsca przechowywania dokumentacji księgowej,
- miejsca zamieszkania, zameldowania osób reprezentujących podmioty,
- samochody,
- wynajmowane pomieszczenia,
- biura rachunkowe, księgowe,
- i wiele innych miejsc.

Formy zabezpieczenia:

- pakiet – metoda pozwalająca na skrócenie czasu czynności przeszukania, ale utrudniająca wykonywanie czynności później i szybkiego wykorzystania materiału dowodowego zgromadzonego w pakiecie.
- pojedyncze dokumenty (czasochłonne) – do wykorzystania jedynie w trakcie przeszukań, których celem jest zabezpieczenie już wcześniej wyselekcjonowanych dokumentów,
- zaplombowane segregatory – metoda pozwalająca na szybkie zabezpieczenie materiału, a także na późniejszy bezproblemowy dostęp do niego,
- ponumerowane segregatory – czasochłonne, nie wykluczające pomyłek przy zabezpieczeniu.

Wybrane „problemy" na jakie natrafiamy przy prowadzeniu tego rodzaju śledztw:

- tajemnice (adwokacka, radcowska, notarialna, obrończa, doradcy podatkowego, biegłego rewidenta, lekarska, psychiatryczna, pielęgniarki i położnej, aptekarska, dziennikarska, komornicza, skarbowa, celna, pracownika kontroli skarbowej, rzecznika patentowego, rzeczoznawcy majątkowego, sędziowska, prokuratorska, giełdowa, giełdy towarowej, maklerska, brokerska, funduszy inwestycyjnych, funduszy emerytalnych, ubezpieczeniowa, pośredników ubezpieczeniowych, informacji niejawnych, funkcyjna, spowiedzi, statystyczna,

korespondencji, posła i senatora, komisji śledczej, przedsiębiorstwa, geologiczna, dawcy krwi, postępowania karnego, własności przemysłowej i in., psychologa, pocztowa, bankowa, telekomunikacyjna, ZUS),
- braki szkoleniowe,
- brak doświadczenia śledczego w Administracji Skarbowej,
- ogrom dokumentów, konieczność oględzin, procedury związane z dowodami rzeczowymi,
- wielość podmiotów uczestniczących w przestępstwie, wielość dokumentów o charakterze dowodowym poddawanych ekspertyzom, ogólnokrajowy i (lub) transgraniczny charakter czynów, wielość kontroli skarbowych,
- problemy wynikające z faktu współwystępowania przestępstw powszechnych (art. 258 k.k., art. 299 k.k.),
- niewydolność komórek analitycznych,
- koszty opinii biegłych w tym biegłych informatyków,
- brak współpracy i niechęć do współpracy,
- wiele służb zajmująca się tematyką i brak koordynacji.

Czynności o charakterze operacyjnym:
Mogą:
- poprzedzać postępowanie przygotowawcze,
- być prowadzone równolegle,
- trwać po zakończeniu postępowania przygotowawczego.

Formy i metody:
- właściwe dla poszczególnych służb, wymienione w aktach prawnych o charakterze niejawnym,
- przewidziane w jawnych aktach prawnych, np. ustawie o Policji: kontrola korespondencji, kontrola operacyjna, przesyłka niejawnie nadzorowana,
- analiza kryminalna jest doskonałym narzędziem dla prawidłowego ustalenia stanu faktycznego, nie tylko pozwala na ustalenia w zakresie przepływu środków jak i towarów, ale także pozwala na ustalenie siatki powiązań, osób jak i podmiotów. Bieżąca, pełna współpraca pomiędzy analitykiem a innymi prowadzącymi czynności, czy to procesowe czy operacyjne, pozwala ukierunkować bieg śledztwa, znacznie je skrócić, czy doskonale wytypować źródła i środki dowodowe.

Jak ważne jest prowadzenie czynności o charakterze operacyjnym, równoległe do czynności o charakterze procesowym, pokazują aktualne Wytyczne Prokuratora Generalnego nr 5/2017 z dnia 10 sierpnia 2017 r. w sprawie zasad prowadzenia postępowań przygotowawczych w sprawach o przestępstwa związane z procederem wyłudzania nienależnego zwrotu podatku od towarów i usług (VAT) oraz innych oszukańczych uszczupleń w tym podatku, gdzie w pkt. 5 wskazane jest „aby w uzasadnionych przypadkach, czynności operacyjno-rozpoznawcze (w tym kontrola operacyjna) prowadzone były również w trakcie postępowania przygotowawczego, zwłaszcza na jego wstępnym etapie. Należy w tym zakresie dokonywać

stosownych uzgodnień z organami uprawnionymi do realizowania takich czynności, a jeżeli osiągnięcie porozumienia okaże się niemożliwe, w szczególnie uzasadnionych wypadkach należy występować do Prokuratora Generalnego z wnioskiem o skorzystanie przez niego z uprawnień przewidzianych w art. 57 § 3 Prawa o prokuraturze. Informacje uzyskane w toku czynności operacyjno-rozpoznawczych powinny być przekazywane prokuratorowi na bieżąco, w celu ich wykorzystania w toku prowadzonego postępowania. Ponadto, w razie spełnienia przesłanek z art. 237 k.p.k., rozważyć należy zarządzenie przewidzianej w tym artykule kontroli i utrwalania treści rozmów telefonicznych."

Jak mówi praktyka, skomplikowane prowadzenie czynności o charakterze procesowym, w szczególności w sprawach o przestępstwa „karuzelowe", musi przebiegać równolegle, przy pełnej transparentności, z prowadzeniem czynności o charakterze operacyjnym. Tylko przenikanie się zakresów i uprawnień tych dwóch rodzajów czynności pozwalają na osiągnięcie sukcesów w zwalczaniu tego rodzaju przestępczości.

Mjr. Michał Pudło

Intelligent Department Central Bureau of Investigation of the Police Regional Office in Katowice

Preparatory proceedings with the use of operational work in cases regarding carousel fraud – practical aspects

Abstract

The growing VAT gap, which is caused mainly by tax fraud, has taken on proportions that endanger the economic security of the State. Tax shortfalls endanger also the security of economic trade through violating the principles of fair competition. In consequence, they may lead to driving fair undertakings out of the market as they are unable to effectively compete with businesses „subsidised" from taxes obtained through criminal activities.

The so-called „carousel fraud" is the most serious fiscal crime in the entire European Union. For the mechanism to be profitable, an entity or entities involved in the so-called „chain of transactions" do not pay due VAT while the other unduly reclaims it. Combating this type of organised crime requires full cooperation between services competent for dealing with fiscal crime and combating organised crime.

Complex procedural activities must be conducted concurrently, and with full transparency, with operational activities. Success in combating this sort of crime is possible only if the respective scopes and remits of these two types of activities overlap.

The growing VAT gap, which is caused mainly by tax fraud, has taken on proportions that endanger the economic security of the State. Tax shortfalls endanger also the security of economic trade through violating the principles of fair competition. In consequence, they may lead to driving fair undertakings out of the market as they are unable to effectively compete with businesses „subsidised" from taxes obtained through criminal activities.

The so-called „carousel fraud" is the most serious fiscal crime in the entire European Union. For the mechanism to be profitable, an entity or entities involved in the so-called „chain of transactions" do not pay due VAT while another entity unduly reclaims it. Therefore, a part of the practice must involve the so-called „missing traders – front companies", or persons who issue invoices that are not reflected in actual transactions and do not pay taxes due under the issued documents. In practice, „carousel fraud" is organised, hierarchically structured, large scale crime that endangers the foundations of public finances. The practice is most often aimed at extorting VAT which in fact has never been paid, but also at evading taxes. „A carousel" can also be used to place goods from unknown sources (e.g. smuggling) on the market or legalise financial funds i.e. money laundering. Also, the practice allows perpetrators to lower prices for goods in order to offer these goods on the domestic market at prices that are competitive to undertakings that sell identical goods but operate legally.

There are around 100 investigations in progress in Poland at present (these are the most serious ones where the value of shortfalls or undue VAT refunds exceeds PLN 1 million) and the total amount of shortfalls in public-law liabilities, as identified in preparatory proceedings, is now PLN 5 billion. It should be highlighted that majority of the investigations relate to criminal activities from previous years i.e. between 2010 and 2014.

Combating this type of organised crime requires full cooperation between services competent for dealing with fiscal crime and combating organised crime.

The term „tax carousel" applies to the manner in which goods are passed around respective traders involved in the fraud. The goods are different – from fuel to gold. Most of them are expensive small items that are popular on the market, which makes them easy to sell. This allows the fraudster to generate large turnover over a short period of time to quickly achieve a high VAT refund. Fraudsters use goods that are relatively easy to be moved between companies. Practice shows that the largest fraud cases take place in the trade of fuel, scrap metals, mobile phones, electronics and computers and applications for smartphones and tablets.

Crime groups quickly change market sectors – when we create unfavourable conditions for their operations in one, they immediately move to another. The scrap sector was an example here. After the VAT reverse charge method had been introduced, fraudsters moved to other goods like e.g. steel.

The State is unable to change regulations quickly enough to eliminate fraud in the entire spectrum of a given sector. The higher the value of specific goods, the larger the associated VAT refunds.

Entities involved in tax carousels

„Front" or a missing trader – an entity used for creating an impression of genuine operations in intra-community transactions made in order to fraudulently obtain profit on VAT charged on the next transaction;

Characteristic features:

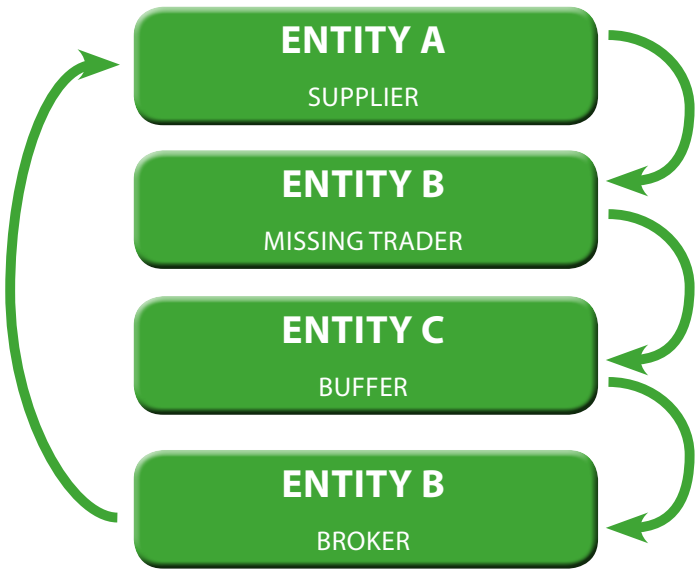
- does not meet his/her tax obligations – does not pay the tax or submit tax returns. If he/she submits tax returns, they are the so-called „nil returns",
- operates for a short time (up to around 20 months),
- does not actually run business (he/she either only provides an address or the address is false),
- does not have any assets or means to run business,
- makes intra-Community acquisitions of goods and domestic supplies for a buffer undertaking or broker,
- to deceive tax authorities, he/she may make intra-Community supplies of goods in addition to domestic supplies.
- often a limited liability company (Sp. z o.o.) – members of the management board are either dummies or foreign companies are registered in the so-called „tax havens" (tax administration does not have access to their documents).

„Broker", also referred to as „VAT Provider", „VAT Sponsor", „Operator" – a company which is the final link and one of the recipients of the fraudulent profit; situated in the same EU Member State as the missing trader; purchases the goods and/or services from the buffer and supplies them to a foreign entity as part of intra-Community supplies of goods; the entity that makes the purchase from the buffer (rarely the missing trader) and an intra-Community supply of goods to the leading company or a domestic supply to the domestic market.

Characteristic features:

- submits VAT refund application for purchases made or pays a small surplus of the tax over the input tax,
- the broker may act as a buffer, e.g. make transactions related to the fraud to other entities in the same Member State,
- sometimes he/she is so-called „leading entity" i.e. the key entity and organiser of carousel fraud; he/she makes an impression of complying with regulations and acting in good faith; he/she has the capital and resources to run business in a trustworthy manner,
- keeps correct accounting; submits tax returns and timely pays public its law liabilities (usually in small amounts though),
- he/she is an entity registered in the same Member State where the missing trader operates.

Foreign entity – most often a Czech or Slovak entity, used for the so-called „VAT zeroing". Goods and sales invoices from Polish entities – company referred to as operators, VAT beneficiaries or VAT providers (with 0% VAT rate due to intra-Community supplies of goods) are apparently sold to this entity and then the goods apparently return to Poland based on invoices to further links in the „VAT carousel" (at a 0% VAT rate), the so-called „front" companies – missing traders, from whom they are transferred (at a 23% VAT rate) to the so-called „buffers". The owners or management board members in such Czech or Slovak entities are Polish nationals.



Operating diagram of tax carousel

Evidence gathering – first procedural activities

To ensure the appropriate course of the investigation activities, it is necessary to systematically gather information on business entities that are involved in the fraud, including data from:

- the revenue administration,
- ZUS (Social Security),
- National Court Register or business register,
- bank accounts,
- telecommunications data,
- other sources (licences, permits etc.)

It is also necessary to, from the very start, systematically gather information on individuals (PESEL, CBA, bank accounts). Data and information should be gathered in a manner that provides for quick location and use. This can be facilitated by analytical tools, not only professional ones, like those used for criminal analysis, but also basic calculation sheets.

Seizure of financial and accounting documentation

The documentation must include flows of goods (e.g. CMR, warehouse documents, transport documents), trade documentation (invoices, agreements), cash flows (bank documentation, cash documentation). Also, and perhaps more importantly, electronic versions of such documentation should be seized. This will significantly facilitate and accelerate further activities, including analytical activities.

Most common errors in seizing of documents:

- only invoices are seized, without transport or payment documentation,
- transport documents (CMR) are seized without analysing or further checks at the carriers,
- no bank documentation is seized other than that supplied by the Inspector General of Financial Information (GIIF), which is often rudimentary; no requests are filed for history of bank accounts based on new documentation seized in the case concerned.
- no electronic versions of the documentation are seized.

Key documents to be seized:

- invoices,
- CMRs,
- VAT sales and purchases register,
- tax return,
- warehouse documents,
- bank accounts,
- documents like proofs of payment (KP) or journal voucher (DW) and other cash documentation,
- payment cards,
- notarial deeds,
- notes, diagrams.

Where to search:

- places of business,
- places where accounting documentation is stored,
- places of residence/registration of representatives of the entities concerned,
- vehicles,
- leased premises,
- accountancy offices,
- and many other places.

Forms of seizure:

- package – a method that provides for reducing the time of search but hinders subsequent activities and quick use of the evidence gathered in a package.
- single documents – time consuming, to be employed only during searches aimed at seizing pre-identified documents,
- sealed binders – a methods that provides for quick seizure of evidence and subsequent easy access to it,
- numbered binders – time consuming, possible mistakes in the process of seizure.

Selected „problems" faced during investigations of this type:

- secrets (professional privileges: legal, attorney, notary, defence, tax advisor, auditor, doctor, psychiatrist, nurse and midwife, pharmacist, journalist, bailiff, revenue office, customs, revenue control employee, patent attorney, property valuer, judge, prosecutor, stock exchange, commodity exchange, broker, stockbroker, investment funds, pension funds, insurance, insurance agents, classified information, function-related, religious confession, statistical, correspondence, Member of Parliament and Senator, investigating committee, trade secret, geological, blood donor, criminal proceedings, industrial and other property, psychologist, mail, bank, telecommunications, Social Insurance Institution),
- lacks in training,
- an investigator without experience in Revenue Administration,
- multitude of documents, necessity to inspect, procedures related to material evidence,
- multiple participants in the crime, multitude of evidence documents to be examined, nationwide and/or cross-border nature of the crime, multiple revenue audits,
- problem arising from the fact of coexistence of common offences /Article 258 of the Penal Code, Article 299 of the Penal Code/,
- inefficiency of analytical units,
- costs of expert opinions, including IT experts,
- no cooperation or willingness to cooperate,
- multiple services dealing with the case – lack of coordination.

Activities of operational nature:

They can:

- precede the preparatory proceedings,
- be conducted concurrently,
- continue after completion of the preparatory proceedings.

Forms and methods:

- specific to respective services, listed in non-public legal acts,
- set out in public legal acts, e.g. the Police Act: surveillance of correspondence, operational control, controlled delivery.
- criminal analysis is an excellent tool for correct identification of facts; not only does it provide for identifying flows of funds and goods, but also for identifying a network of connections between individuals and entities. On-going full cooperation between an analyst and other officers conducting procedural or operational activities provides for focusing the course of the investigation, shorten it significantly and excellently pinpoint evidence sources and measures.

The great importance of conducting operational activities concurrently with procedural activities is shown in Guidelines No. 5/2017 of the Prosecutor General of 10 August 2017 on the rules of conducting preparatory proceedings in cases regarding crimes related to the practice of extorting undue VAT refunds and other fraudulent tax shortfalls, where it is stated in Point 5 that „when justified, operational and exploratory activities (including operational control) should be conducted also during the preparatory proceedings, especially at its early stage. In this respect, arrangements should be made with authorities authorised to conduct such activities, and is such arrangements are not possible, then, in particularly justified cases, the Prosecutor General should be requested to use his her authority as set out in Article 57 § 3 of the Prosecution Service Law. Information obtained in the course of operational and exploratory activities should be delivered to the prosecutor on an on-going basis so that it could be used in the course of the proceedings. Moreover, if Article 237 of the code of criminal procedure is satisfied, control and recording of telephone calls, as provided for in the said Article, should be considered."

As shown by practice, the complex procedural activities, particularly in „carousel fraud" cases, must be conducted concurrently, and with full transparency, with operational activities. Success in combating this sort of crime is possible only if the respective scopes and remits of these two types of activities overlap.

Monika Duda-Szmyd
Wydział Europejskiego Funduszu Rozwoju Regionalnego – Urząd Marszałkowski Województwa Śląskiego

Błędy i nieprawidłowości w wydatkowaniu środków finansowych w projektach realizowanych w ramach RPO WSL 2007-2013

Streszczenie

Referat omawia realizację Regionalnego Programu Operacyjnego Województwa Śląskiego na lata 2007-2013 zgodnie z zasadami zawartymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) NR 1083/2013 z dnia 11 lipca 2006 r., a także na poziomie krajowym w ustawie z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju.

Przedstawiono kolejne etapy procesu udzielania wsparcia podmiotom aplikującym o środki unijne, a także jak przebiegała weryfikacja kwalifikowalności wydatków.

W wyniku kontroli najwięcej nieprawidłowości stwierdzano w obszarze zamówień publicznych.

W ramach perspektywy unijnej 2007-2013 Regionalny Program Operacyjny Województwa Śląskiego na lata 2007-2013 był realizowany przez województwo śląskie pełniące rolę Instytucji Zarządzającej. Rola i funkcje Instytucji Zarządzającej zostały opisane w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) NR 1083/2013 z dnia 11 lipca 2006 r., a także na poziomie krajowym w ustawie z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju. Doprecyzowanie roli i zadań również znalazło się w innych dokumentach, które stanowiły niejako zbiór zasad dotyczących wdrażania funduszy unijnych. Do tego obszaru należały wytyczne wydawane przez Ministra Rozwoju Regionalnego, rozporządzenia krajowe, ustawa o finansach publicznych , a także wiele rozporządzeń unijnych wydawanych w związku z zagadnieniami problemowymi występującymi w obszarze przekazywania środków unijnych.

Proces udzielania wsparcia podmiotom aplikującym o środki unijne przebiegał wieloetapowo. Poczynając od oceny wniosku o dofinansowanie składanego do Instytucji, wybór dofinansowania, podpisania umowy o dofinansowanie projektu oraz jej dalszej realizacji, rozliczenia finansowego projektu, wypłatę dofinansowania oraz monitorowanie celu i wskaźników projektu po jego zakończeniu. Finansowanie projektu polegało na częściowym sfinansowaniu wydatków kwalifikowalnych. Na etapie oceny wniosku o dofinansowanie dokonywana jest ocena kwalifikowalności planowanych wydatków. Przyjęcie danego projektu do realizacji i podpisanie z beneficjentem umowy o dofinansowanie nie oznacza, że wszystkie wydatki, które beneficjent przedstawi we wniosku o płatność w trakcie realizacji projektu zostaną

poświadczone, zrefundowane lub rozliczone. Dodatkowo, jak wskazują postanowienia wytycznych horyzontalnych, ocena kwalifikowalności poniesionego wydatku dokonywana jest przede wszystkim w trakcie realizacji projektu poprzez weryfikację wniosków o płatność oraz w trakcie kontroli projektu. Ocena kwalifikowalności poniesionych wydatków jest prowadzona także po zakończeniu realizacji projektu w zakresie obowiązków nałożonych na beneficjenta umową o dofinansowanie oraz wynikających z przepisów prawa.

Weryfikacja kwalifikowalności wydatków była prowadzona poprzez ocenę poniesionych wydatków przedstawionych we wniosku beneficjenta o płatność, kontrolę doraźną projektu, kontrolę projektu w miejscu jego realizacji, kontrolę krzyżową, informacje pozyskane od podmiotów zewnętrznych, weryfikację dokumentów na etapie rozliczania umowy, a także kontrolę trwałości projektu po zakończeniu jego realizacji.

Uznanie wydatków za niekwalifikowalne na którymkolwiek etapie wiązało się ze stwierdzeniem nieprawidłowości, która została zdefiniowana w rozporządzeniu ogólnym. Nieprawidłowość to jakiekolwiek naruszenie przepisu prawa wspólnotowego wynikające z działania lub zaniechania podmiotu gospodarczego, które powoduje lub mogłoby spowodować szkodę w budżecie ogólnym Unii Europejskiej w drodze finansowania nieuzasadnionego wydatku z budżetu ogólnego. Jak widać z treści definicji, nie musiało dojść do rzeczywistej szkody finansowej, aby została stwierdzona nieprawidłowość. Wystarczyło stwierdzenie naruszenia przepisów prawa, które nawet potencjalnie mogło doprowadzić do uszczerbku.

Obszary, w których identyfikowano najwięcej naruszeń skutkujących pomniejszeniem wypłaconego dofinansowania występowały w zakresie:

- nieprzestrzegania prawa zamówień publicznych,
- finansowania podatku od towarów i usług (VAT),
- pomocy publicznej,
- nieprzestrzegania wytycznych,
- poniesienia wydatku niezgodnego z umową,
- niezrealizowania celu projektu,
- nieosiągnięcia wskaźników projektu,
- wydatkowania środków zaliczki na pokrycie wydatków nieobjętych umową,
- nieutrzymania trwałości projektu.

Z podanych obszarów ewidentnie najwięcej nieprawidłowości stwierdzano w obszarze zamówień publicznych.

Monika Duda-Szmyd

European Regional Development Fund – Marshal Office Silesian Voivodeship

Errors and irregularities in spending financial funds in projects implemented as part of the 2007-2013 Regional Operational Programme for the Silesia Province (RPO WSL 2007-2013)

Abstract

This paper discusses the implementation of the 2007-2013 Regional Operational Programme of the Silesia Province in accordance with the rules set out in the Regulation (EU) 1083/2013 of the European Parliament and of the Council of 11 July 2006, and on the national level - in the Act of 6 December 2006 on the principles of development policy.

Verification of the expenditure eligibility and the process of providing support to entities applying for EU funds, which involved a number of phases, was outlined.

A majority of irregularities was detected in the area of public procurement as a result of various project checks and project control..

Under the 2007-2013 EU perspective, the 2007-2013 Regional Operational Programme of the Silesia Province was implemented by the Silesia Province as the Managing Authority. The role and functions of the Managing Authority are set out in Regulation (EU) 1083/2013 of the European Parliament and of the Council of 11 July 2006, and on the national level - in the Act of 6 December 2006 on the principles of development policy. More precise definitions of the role and tasks were included also in other documents, which made up a set of principles regarding implementation of EU funds. They included guidelines issued by the Minister of Regional Development as well as national Regulations, the Public Finance Act and numerous EU Regulations regarding issues related to transfer of EU funds.

The process of providing support to entities applying for EU funds involved a number of phases including assessment of applications for funding, selection of successful applicants, signature of funding agreements, implementation of the agreements, financial settlement of the financed projects, payouts of the funding and monitoring of the project objective and indicators after the project completion. Funding of a project consisted in partial funding of the eligible expenditure. At the funding application assessment phase, the planned expenditure is analysed for eligibility. Acceptance of a specific project and signature of the related funding agreement with the beneficiary does not mean that all expenditure presented by the beneficiary in the application will be certified, reimbursed or cleared. Additionally, as stipulated by the horizontal guidelines, assessment of the eligibility of a specific expenditure

is conducted primarily at the project implementation phase by means of verification of the payment applications and during the project control. The expenditure eligibility assessment is conducted also after the project has been completed and it regards the obligations imposed on the beneficiary under the relevant funding contract and applicable provisions of law.

The expenditure eligibility was verified by reference to the incurred expenditures shown in the beneficiary's payment application and by means of ad hoc project checks, on-site project checks, cross checks, information obtained from external entities, verification of documents at the contract settlement phase and control of the sustainability of the project after its completion.

Expenditures were considered as illegible at any stage if any irregularities were found as defined in the General Regulation. The term "irregularity" means any breach of Union law resulting from an act or omission by an economic undertaking, which has, or would have, the effect of prejudicing the general budget of the European Union by charging an unjustified item of expenditure to that budget. As evident from the definition, no actual financial prejudice had to occur for an irregularity to be identified. Indeed, it was sufficient to identify a breach that would have led to a potential prejudice.

Areas where the greatest number of breaches were identified:

- resulting in reducing the funding paid,
- regarded non-compliance with the public procurement law,
- VAT financing,
- public aid,
- non-compliance with the guidelines,
- incurring an expenditure in conflict with the contract,
- failure to achieve the objective of the project,
- failure to achieve project indicators,
- spending of pre-financing on expenditures not covered by the contract,
- failure to maintain the project sustainability.

Of the aforementioned areas, a clear majority of irregularities was detected in the area of public procurement.

mł. insp. Piotr Trzciński
Wydział ds. Odzyskiwania Mienia Biura Kryminalnego Komendy Głównej Policji

Konfiskata rozszerzona oraz nowe uprawnienia polskich organów ścigania w zwalczaniu przestępczości zorganizowanej zmierzające do ujawnienia i konfiskaty nielegalnych dochodów

Streszczenie

Przedmiotem wystąpienia będzie prezentacja istotnych zmian prawa karnego oraz niektórych ustaw branżowych w obszarze odzyskiwania mienia pochodzącego z przestępstw, ze względu wpływu jakie wywiera na działania organów ścigania w czynnościach wykrywczych ukierunkowanych na ujawnienie mienia i korzyści pochodzących z przestępstw.

Nowela ustaw Kodeks postępowania karnego, Kodeks karny, Kodeks postępowania karnego oraz ustawy o Policji weszła w życie 27 kwietnia 2017 roku, pod nazwą aktu ustawa z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (DzU. z 2017 r. poz. 768). Ustawodawca wprowadził do polskiego prawa karnego nową instytucję szeroko rozumianą jako „konfiskata rozszerzona".

Do najważniejszych zmian należą nowelizacje przepisów w obszarze działań operacyjno-rozpoznawczych ukierunkowanych na ujawnienie mienia podlegającego przepadkowi. Doniosłe znaczenie mają zmiany w przepisach delegujących uprawnienia odpowiednich służb w pozyskiwaniu informacji o charakterze majątkowym stanowiących tajemnicę zawodową lub chronioną inną ustawą.

Omawiana nowela prawa karnego i niektórych ustaw w zakresie ujawniania, odzyskiwania i dorowadzenia do zabezpieczenia majątku podlegającego przepadkowi znacząco poprawi i przyspieszy proces wykrywczy organów ścigania a także umożliwi szybszą realizację podstawowego postulatu polskiego prawa karnego procesowego jakim jest restytucja przestępstwa i zapewnienie gwarancji procesowych pokrzywdzonego.

Zwalczanie przestępczości, w tym tej najgroźniejszej o charakterze zorganizowanym, jest możliwe nie tylko poprzez ustalenie i osądzenie samych sprawców, ale również poprzez pozbawienie motywacji do działania przestępczego. Główną motywacją jaka przyświeca większości sprawców przestępstw oraz wszelkim organizacjom przestępczym jest chęć osiągnięcia zysku, a tym samym uczynienia z tego procederu stałego dochodu. Niebagatelną rolę pozbawienia korzyści pochodzących z przestępstw można zaobserwować podczas działań organów ścigania wymierzonych w zwalczanie przestępczości zorganizowanej o wymiarze transgranicznym, ponieważ uderza w wieloaspektową podstawę funkcjonowania grup przestępczych. Głównym motorem jasno wynikającym z motywacji sprawców czynów zabronionych jest możliwość odniesienia stałej korzyści majątkowej. Jest to swoisty sposób na życie. Im bardziej opłacalny, tym bardziej motywujący do wstępowania w szeregi

zorganizowanych grup przestępczych. Finansowa niezależność, szybkość wzbogacenia, jest nieodłącznym elementem osiągania celów nie tylko w prawidłowej gospodarce, ale także w szarej strefie, gdzie majątek może dać poczucie bezpieczeństwa i władzy[1].

Wraz ze zmianami i ewoluowaniem objawów przestępczości organy ścigania starają się dostosować działania karno-procesowe oraz operacyjno-rozpoznawcze do nowych warunków. Ciągłe poszukiwania przez sprawców przestępstw coraz to nowszych mechanizmów ukrywania środków finansowych (korzyści) zmusza instytucje odpowiedzialne za zwalczanie przestępczości do wdrażania nowych elementów prawnych oraz taktyki w wykrywaniu i zabezpieczeniu nielegalnego majątku.

Ostatnia inicjatywa organów wymiaru sprawiedliwości została ukierunkowana na stworzenie warunków prawnych do skuteczniejszego pozbawiania sprawców przestępstw korzyści pochodzących z czynów zabronionych poprzez wprowadzenie nowych środków karnych o charakterze majątkowym, jak również na usprawnienie uzyskiwania informacji o charakterze majątkowym w prowadzonych sprawach przez funkcjonariuszy organów ścigania. W zamierzeniu twórców zmian przepisów prawa karnego oraz ustaw regulujących działalność służb policyjnych było przygotowanie projektu kompleksowych norm prawnych ukierunkowanych na ujawnienie mienia i korzyści pochodzących z przestępstw.

Efektem prac legislacyjnych jest nowela ustaw: Kodeks postępowania karnego, Kodeks karny, Kodeks postępowania karnego oraz ustawy o Policji, która weszła w życie 27 kwietnia 2017 roku, pod nazwą: ustawa z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (DzU. z 2017 r. poz. 768).

Ustawodawca wprowadził do polskiego prawa karnego nową instytucję szeroko rozumianą jako „konfiskata rozszerzona". Wymienionym pojęciem określono zbiór całkiem nowych instytucji prawnych, jak też znowelizowanie dotychczasowych przepisów Kodeksu karnego i Kodeksu postępowania karnego w obszarze stosowania środków karnych o charakterze majątkowym oraz procedury zabezpieczenia mienia na poczet przyszłego orzeczenia sądowego w przedmiocie stosowania tych środków.

Pojęcie „konfiskata" nie jest wprost wyrażone jako środek karny, a także w obecnym kształcie prawa karnego nie funkcjonuje jej legalna definicja. W ramach zmian ustawowych wprowadzono możliwość orzekania środka karnego, a raczej już jako środka prawnego zmierzającego do realizacji podstawowych celów procesu karnego w postaci przepadku przedsiębiorstwa, co jest nowym rozwiązaniem w restytucji przestępstwa. Oprócz charakteru wyrównania czy naprawienia powstałej szkody ma on charakter prewencyjny. Służy realizacji wycofania z rynku przedsiębiorstwa należącego lub nienależącego do sprawcy, które służyło do popełnienia przestępstwa w postaci jego przepadku albo równowartości, jeżeli przedsiębiorstwo służyło do popełnienia tego przestępstwa lub ukrycia osiągniętej z niego korzyści. Potencjalne zagrożenie przepadkiem mienia przedsiębiorstwa pełni także funkcję odstraszenia ewentualnych zamiarów użycia prosperującej firmy w obrocie przestępczym. Podstawowymi przesłankami umożliwiającymi zastosowanie wskazanej instytucji prawnej

[1] Opracowanie własne – P. Trzciński, *Funkcja Scentralizowanego Pionu Policji w pozbawianiu sprawców korzyści finansowych z przestępczości zorganizowanej w: Wspólny Rynek nie tylko dla przestępców – SP Katowice 2011.*

w procesie karnym jest zebranie danych lub dowodów wskazujących, że przedsiębiorstwo służyło do popełnienia przestępstwa lub ukrycia osiągniętej z niego korzyści. Nie jest istotne, czy firma była stworzona od początku na rzecz działań przestępczych czy w trakcie legalnej działalności została do tego wykorzystana. W tym miejscu można podkreślić istotną rolę podmiotów gospodarczych tworzonych w celu kreowania „karuzel podatkowych VAT" czy wykorzystywanych do prania pieniędzy. W przypadku braku, ukrycia lub innego zniweczenia możliwości orzeczenia przepadku przedsiębiorstwa, przewidziano zastosowanie tego środka wobec innego mienia stanowiącego równowartość przedsiębiorstwa objętego przepadkiem. Podobnie jest w przypadku oceny pochodzenia korzyści. Nie jest wymagane, by korzyść była bezpośrednim nielegalnym dochodem, wystarczy że sprawca pośrednio ją uzyskał na przykład poprzez konwersję środków finansowych lub osiągnięcie pożytków. Jako jeden z podstawowych warunków określono poziom, od którego ma zastosowanie przepadek. Korzyść choćby pośrednia osiągnięta przez sprawcę w przypadku przestępstw określonych w Kodeksie karnym powinna wynosić co najmniej 200.000 zł zgodnie z definicją „mienia znacznej wartości"[2]. W przypadku przestępstw skarbowych sytuacja ta dotyczy korzyści z uszczupleń Skarbu Państwa o dużej wartości tj. ok. 1.000.000 zł[3]. Kolejną przesłanką do stosowania przepadku w sytuacji, gdy przedsiębiorstwo nie należy do sprawcy, a należy do innej osoby fizycznej jest wykazanie, że jego właściciel chciał, aby przedsiębiorstwo służyło do popełnienia tego przestępstwa lub ukrycia osiągniętej z niego korzyści albo przewidując taką możliwość na to się godził. Spełnienie wykazania tej przesłanki nie jest wymagane, gdy przedsiębiorstwo należy do samego sprawcy przestępstwa. Poważnym problemem w praktycznym stosowaniu nowych przepisów może stać się ograniczenie ich stosowania do podmiotu z jasno określonym właścicielem w postaci osoby fizycznej. Ustawodawca przewidział jedynie stosowanie przepisów o przepadku do przedsiębiorstwa, które należy do osoby fizycznej, co wydaje się problematyczne przy założeniu występowania w większości przypadków obrotu przestępczego przedsiębiorstw w postaci spółek prawa handlowego, takich jak spółki z ograniczoną odpowiedzialnością lub spółek notowanych na giełdzie papierów wartościowych, gdzie podmioty te posiadają własny byt prawny i osobowość prawną. W ramach wyjątków prawnych ustawodawca przewidział sytuacje, w których organ procesowy może odstąpić od zabezpieczenia, a sąd od wydania orzeczenia o przepadku przedsiębiorstwa. Do takich sytuacji należą wykazane w postępowaniu dowodowym okoliczność obiektywne podyktowane zasadami współżycia społecznego i gwarantujące obronę przez nadmierną represyjnością prawną. Należą do nich sytuacje niewspółmierne, tj. stosunek wagi popełnionego przestępstwa, stopnia zawinienia oskarżonego lub motywacji i sposobu zachowania się właściciela przedsiębiorstwa. Ogólnie wnioskując decydują o tym naruszenia zasad staranności przez właściciela przedsiębiorstwa. Właścicielowi przedsiębiorstwa zagrożonego przepadkiem przysługują prawa strony w zakresie czynności procesowych odnoszących się do tego środka[4]. Podobnym

[2] Art. 115 par. 5 – ustawa Kodeks karny, Dz.U. 1997 Nr 88 poz. 553.

[3] Art. 53 § 15 – ustawa Kodeks karny skarbowy, Dz.U. 1999 Nr 83 poz. 930 – *Duża wartość jest to wartość, która w czasie popełnienia czynu zabronionego przekracza pięćsetkrotną wysokość minimalnego wynagrodzenia.*

[4] Art. 91b cyt. ustawy Kodeks postępowania karnego.

przypadkiem wyłączającym stosowanie instytucji omawianego środka prawnego jest niewspółmierność szkody do stosowania przepadku. Jeżeli szkoda wyrządzona przestępstwem lub wartość ukrytej korzyści nie jest znaczna wobec rozmiaru działalności przedsiębiorstwa, przepadku się nie stosuje. Jest to zrozumiałe odstępstwo, gdzie zastosowanie tak radykalnych środków prawnych może spowodować poważniejsze konsekwencje niż wielkość rozmiaru szkody spowodowany działaniem sprawcy. Również w innych, szczególnie uzasadnionych przypadkach, sąd ma możliwość odstępstwa od zasady, kiedy przepadek przedsiębiorstwa byłby niewspółmiernie dolegliwy dla właściciela. Odstępstwo to ma charakter fakultatywny, uzależniony od stopnia oceny dokonanej na podstawie zebranych dowodów i danych o stosunkach majątkowych i rodzinnych oskarżonego. W przypadku zaistnienia powyższych przesłanek negatywnych do zastosowania przepadku, ustawodawca przewidział możliwość realizacji podstawowych celów procesu karnego[5], tworząc dodatkową normę prawną w art. 47 Kodeksu karnego. Zgodnie z nową dyspozycją[6] normującą środki karne sąd może orzec nawiązkę w wysokości do 1.000.000 złotych na rzecz pokrzywdzonego lub Funduszu Pomocy Pokrzywdzonym oraz Pomocy Postpenitencjarnej.

Kolejnym rozwiązaniem należącym do grupy przepisów określonych jako „konfiskata rozszerzona" jest wprowadzenie możliwości stosowania przepadku korzyści majątkowych, choćby pośrednich, w zakresie stosowania domniemania pochodzenia majątku z czynu zabronionego wydłużając okres zaprzeczalności legalności majątku o 5 lat przed popełnieniem pierwszego czynu. W dotychczasowych przepisach prawa karnego istnieje środek karny w postaci przepadku korzyści pochodzących choćby pośrednio z przestępstwa. Praktyka prokuratorsko-sądowa wskazywała, że sprawcy przestępstw starali się prowadzić takie działania, które uniemożliwiłyby organowi procesowemu dochodzenia roszczeń z tytułu osiągniętych korzyści z przestępstwa. Przy zachowaniu nienoszącym znamion czynu prania pieniędzy istnieje szereg możliwości konwersji korzyści, przenoszenia na inne osoby praw majątkowych lub pożytkowania ich w inny sposób. Praktyka śledcza dostarczała podstaw do stwierdzenia, że w wielu przypadkach zwłaszcza spraw wszczętych o przestępstwa wykryte długo po ich popełnieniu nie można definitywnie określić legalności pochodzenia majątku sprawcy. Problem ten dotyczył zwłaszcza zorganizowanej przestępczości, gdzie sprawcy z popełnianych przestępstw i przynależności do związku przestępczego uczynili sobie z tego tytułu stałe źródło dochodu. Naprzeciw temu wprowadzono do systemu prawno-karnego odstępstwo od podstawowej zasady domniemania niewinności, gdzie ciężar udowodnienia winy spoczywa na organie procesowym, a oskarżony nie ma obowiązku dostarczać dowodów własnej winy. Tak zwana zasada „odwrócenia ciężaru dowodowego" polegająca na imperatywnym domniemaniu, że mienie zgromadzone przez sprawcę w okresie od popełnienia pierwszego zarzuconego przestępstwa o wartości znacznej[7] należące do oskarżonego stanowi korzyść z przestępstwa, stała się podstawowym orężem w walce ze zorganizowaną

[5] *Przepisy Kodeksu postępowania karnego mają na celu takie ukształtowanie postępowania karnego, aby (...) przez trafne zastosowanie środków przewidzianych w prawie karnym (...) zostały uwzględnione prawnie chronione interesy pokrzywdzonego* – art. 2 Ustawy Kodeks postępowania karnego, Dz. U. z 1997 r. Nr 89, poz. 555 z późn. zm.

[6] Art. 47 par. 2a ustawy Kodeks karny (wejście w życie 27.04.2017 r.).

[7] Patrz przyp. 2.

przestępczością[8]. Uzupełnienie domniemania o zarzucenie pozorności przeniesienia majątku na inną osobę lub podmiot uniemożliwia sprawcom oddalanie nielegalnie zgromadzonego majątku pochodzącego z przestępczych korzyści od możliwości jego zabezpieczenia i odebrania w celu orzeczenia przepadku. W nowelizacji przepisów dotyczącej przepadku korzyści pochodzących z przestępstwa dokonano poważnych zmian rozszerzających możliwość jego stosowania w wymiarze czasowym co do momentu zgromadzenia majątku, jak też rodzaju przestępstw. Od wejścia w życie noweli ustawy[9] można stosować instytucję domniemania pochodzenia korzyści z przestępstwa, jeśli przestępstwo przynoszące korzyść majątkową jest zagrożone karą pozbawienia wolności, której górna granica jest nie niższa niż 5 lat albo było popełnione w zorganizowanej grupie. W związku z tym organ ścigania może poszukiwać mienia nabytego nawet w ciągu 5 lat przed popełnieniem przestępstwa do chwili wydania nieprawomocnego wyroku w celu jego zabezpieczenia. Sprawca lub inna zainteresowana osoba musi przedstawić dowód przeciwny domniemaniu. Dowód ten poza wszelką wątpliwość powinien wykazywać, że ustalony majątek sprawcy pochodzi z legalnego źródła finansowania. W przypadku przeniesienia pod jakąkolwiek pozornością prawa majątkowego na inną osobę jak to bywa najczęściej w działaniach grup przestępczych uważa się, że przedmioty będące w samoistnym posiadaniu innej osoby faktycznie należą do sprawcy, chyba że na podstawie okoliczności towarzyszących ich nabyciu osoba nabywająca nie mgła przypuszczać, że mienie nabywane stanowi korzyść z przestępstwa.

Ponadto w Kodeksie postępowania karnego wprowadzono nową instytucję żądania zwrotu korzyści przez osobę prawną, która uzyskała taką w wyniku przestępczego działania osoby działającej w jej imieniu[10]. Osobą taką w rozumieniu przepisów może być przedstawiciel lub osoba reprezentująca organ zarządzający i jest wtedy przesłuchany w charakterze świadka w procesie karnym. Na wniosek prokuratora sąd, stosując przepisy prawa cywilnego, zobowiązuje tę osobę lub jednostkę prawną do zwrotu korzyści albo jej równowartości uprawnionemu podmiotowi lub orzeka przepadek świadczenia albo jego równowartości na rzecz Skarbu Państwa. Jest to podobne i znane rozwiązanie z Kodeksu karnego skarbowego[11], które umożliwia dochodzenie zwrotu korzyści ulokowanej w podmiocie prawa handlowego lub innym podmiocie określonym odrębnymi przepisami.

W ramach zmian ustawowych doprecyzowano także przepisy Kodeksu postępowania karnego w zakresie umożliwienia orzeczenia przepadku korzyści również w razie śmierci sprawcy, zawieszenia postępowania lub umorzenia z powodu niewykrycia lub ukrywania się sprawcy. Jest to nowe rozwiązanie polskiej procedury karnej, która obecnie przewiduje możliwość zastosowania przepadku bez wydania wyroku skazującego. Biorąc pod uwagę dalsze aspekty procedowania z zajętą korzyścią pochodzącą z przestępstwa, którą obecnie można po części zaspokoić roszczenia pokrzywdzonego z tytułu wyrównania straty, jest to dobry

[8] Art. 45 par. 1-3 Kodeksu karnego.

[9] Ustawa z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (weszła w życie 27.04.2017 r.).

[10] Do Kodeksu karnego wprowadzono Rozdział 10a – Podmiot zobowiązany.

[11] Art. 24 Ustawy Kodeks karny skarbowy, Dz. U. z 2007 r. Nr 111 z późn. zm.

kierunek zmian umożliwiający w pełni zrealizowanie postulatu restytucji przestępstwa w postaci zagwarantowania interesów pokrzywdzonego[12].

Zmianom legislacyjnym uległy również przepisy stanowiące podstawę stosowania zabezpieczenia majątkowego na poczet przyszłych kar o charakterze majątkowym oraz środków karnych majątkowych lub środków kompensacyjnych. Norma prawna regulująca podstawę stosowania zabezpieczenia majątkowego na mieniu oskarżonego lub podejrzanego w swojej dyspozycji obecnie zawiera enumeratywnie wymieniony katalog środków prawnych. Na uwagę zasługuje ostatni punkt 5 katalogu[13]. Jako możliwość stosowania środków prawnych dodano punkt o treści „zwrot pokrzywdzonemu lub innemu uprawnionemu podmiotowi korzyści majątkowej, jaką sprawca osiągnął z popełnionego przestępstwa albo jej równowartości". Niejako jest to środek prawny do realizacji przeznaczenia części korzyści z przestępstwa zabezpieczony podejrzanemu na rzecz wyrównania straty uprawnionemu, najczęściej samemu pokrzywdzonemu. Oczywiście konsekwentnie dodano zapis o uprawnieniu zabezpieczenia majątkowego na mieniu podmiotu zobowiązanego do zwrotu korzyści[14].

W ramach cytowanej ustawy wprowadzono szereg zmian w ustawach regulujących działanie służb państwowych odpowiedzialnych za wykrywanie i ściganie przestępstw. Do najważniejszych zmian należą nowelizacje przepisów w obszarze działań operacyjno-rozpoznawczych ukierunkowanych na ujawnienie mienia podlegającego przepadkowi. W przepisach uprawniających organy ścigania do stosowania kontroli operacyjnej wprowadzono dodatkową podstawę faktyczną w postaci możliwości jej stosowania oprócz w enumeratywnie wymienionych przestępstwach także w ramach prowadzenia ustaleń majątkowych[15]. Zgodnie z brzmieniem dodanego punktu stanowiącego podstawę faktyczną stosowania kontroli operacyjnej, jeśli działania są ukierunkowane na ujawnienie mienia zagrożonego przepadkiem w związku z przestępstwami zawartymi w punkcie 1-8 art.19 ust. 1 ustawy o Policji, czyli w sprawie poważnych przestępstw, można stosować kontrolę operacyjną. Przy czym działania operacyjne nie ograniczają się jedynie do stosowania ustawowej metody pracy operacyjnej w postaci stosowania podsłuchu telefonicznego czy przykładowo podsłuchu pomieszczeń. Są to wszelkie prawem dozwolone i w jego granicach zachowania organu ścigania stosującego wymienioną metodę, która zawiera się w określeniu ustawowym jako „kontrola operacyjna". Ustawodawca jednak poszedł dalej z uprawnieniem stosowania kontroli operacyjnej odnośnie do ustaleń majątkowych mienia. Oczywiście obostrzył do ustalenia mienia jedynie podlegającego przepadkowi, jednak dodał uprawnienie stosowania jej również o przestępstwa wymienione w art. 45 § 2 k.k. i 33 § 2 k.k.s. W związku z tym do dyspozycji organów ścigania oddano możliwość stosowania metody pracy operacyjnej indywidualnie bez obostrzenia wynikającego z katalogu przestępstw art. 19 ust. 1 pkt. 1-8 ustawy o Policji[16], a co znamienne

[12] Patrz przyp. 4.

[13] Art. 291 par. 1 i 2 w brzmieniu znowelizowanej ustawy, tekst uchwalony – Ustawa z dnia 23 marca 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw.

[14] Szerzej, patrz przyp. 10.

[15] Art. 19 Ust.1 pkt. 9 w brzmieniu znowelizowanej ustawy o Policji, Dz.U. 1990 Nr 30 poz. 179 z późn. zm.

[16] Autor jako przykład podaje przepisy ustawy o Policji, jednak zmiany dotyczą w tym zakresie także ustawy o Straży Granicznej i innych służb.

rozszerzono o możliwość stosowania w sprawach o przestępstwa, których zagrożenie górną granicą pozbawienia wolności wynosi 5 lat oraz przestępstwa, z których sprawca osiągnął znaczną korzyść. Nietrudno w tym miejscu o refleksję, że ustawodawca dał organom ścigania możliwość stosowania zaawansowanej metody pracy operacyjnej w o wiele szerszym zakresie w sprawie ustalenia mienia niż samym dążeniu do wykrycia sprawców i utrwalenia dowodów przestępstwa.

Doniosłe znaczenie mają zmiany w przepisach delegujących uprawnienia odpowiednich służb w pozyskiwaniu informacji o charakterze majątkowym stanowiących tajemnicę zawodową lub chronioną inną ustawą[17]. Obok możliwości pozyskiwania informacji z umów bankowych i ubezpieczeniowych dodano katalog danych pozostających w dyspozycji takich instytucji, jak urzędy podatkowe, zakłady ubezpieczeń powszechnych, instytucje prowadzące domy maklerskie oraz instytucje rynku instrumentów finansowych. Ustawa o Policji jako najgłębiej znowelizowana w tym kierunku dodaje całkiem nowe rozwiązania prawne usprawniające wymianę informacji również z podziałem na kontrolę sądową i bez takiego wymogu w oparciu o elektroniczne systemy wymiany danych. Funkcjonariusz prowadzący czynności operacyjno-rozpoznawcze uzyskał możliwość szybkiego dotarcia do informacji o lokowanych składnikach majątkowych przez figurantów spraw lub osoby podejrzane. Podstawowym kryterium odróżniającym uzyskiwanie informacji z instytucji finansowych oraz innych urzędów i podmiotów jest zakres otrzymywanych informacji w procedurze objętej kontrolą sądową lub bez takiej kontroli. Ustawodawca rezygnując z długiej drogi formalnej poddania kontroli sądowej na rzecz szybkiego otrzymywania informacji jedynie na wniosek uprawnionych kierowników jednostek organizacyjnych, celowo ograniczył zakres danych jakie tą drogą może otrzymać funkcjonariusz[18]. Są to dane pozbawione informacji najbardziej wrażliwych z punktu interesu ich posiadacza lub objęte ważną ochroną ustaw szczególnych. W ocenie autora jest to dobre rozwiązanie mające na celu ustalenie gdzie sprawca lub osoba objęta zainteresowaniem operacyjnym, w związku z popełnieniem przestępstwa, może lokować przestępcze dochody, a brak szybkiego ustalenia i identyfikacji składników majątkowych uniemożliwia ich odzyskanie przy dalszej zwłoce. Jest to również rozwiązanie wysoce przydatne w zwalczaniu przestępczości podatkowej, zwłaszcza tej o charakterze zorganizowanym z wykorzystaniem podmiotów pozorujących prowadzenie działalności gospodarczej takich jak np. „karuzele VAT".

Omawiana nowela prawa karnego i niektórych ustaw w zakresie ujawniania, odzyskiwania i doprowadzenia do zabezpieczenia majątku podlegającego przepadkowi znacząco poprawi i przyspieszy proces wykrywczy organów ścigania a także umożliwi szybszą realizację podstawowego postulatu polskiego prawa karnego procesowego jakim jest restytucja przestępstwa i zapewnienie gwarancji procesowych pokrzywdzonego.

[17] Art. 20 ustawy o Policji zmieniony nowelą (druk 1186 – tekst ustawy ustalony ostatecznie po rozpatrzeniu poprawek Senatu).

[18] Art. 20 Ust. 5b znowelizowanej ustawy.

Lt. Col. Piotr Trzciński

Department of the Criminal Bureau of the National Police Headquarters

Extended Confiscation and new rights of Polish law enforcement agencies in combating organised crime aimed at identifying and confiscating of unlawful profits

Abstract

The author will present important changes to criminal law and certain sector-related acts related to recovery of illegally gained assets in the context of their influence on detection activities of law enforcement agencies aimed at disclosing of unlawfully obtained assets and benefits.

The set of amendments to the Code of Criminal Procedure, Criminal Code and the Police Act entered into force on 27 April 2017 under the Act of 23 March 2017 on amending the Act of the Code of Criminal Procedure and certain other Acts (Journal of Laws 2017, Item 768). The legislator introduced a new measure, broadly understood as "extended confiscation", to the Polish legal system.

The most important of those changes include the amendment to the provisions on operational and exploratory activities aimed at disclosing property subject to forfeiture.

Significant changes were introduced in the provisions on the rights of respective services to acquire property-related information protected by professional privileges or other Acts.

The Police Act, which received the widest reaching amendments in this respect, features new legal solutions that facilitate exchange of information through electronic data exchange systems with and without a judicial review.

The aforementioned amendments to the criminal law and other Acts regarding disclosure, recovery and seizure of assets subject to forfeiture will significantly improve and accelerate the detective processes within law enforcement agencies and provide for faster implementation of the primary postulate of the Polish procedural criminal law regarding restitution of the crime and procedural guarantees for the victim.

Crime, also the most dangerous organised crime, can be combated not only through identifying and sentencing perpetrators themselves by also by eliminating the motivation to commit crime. The key motivation that drives majority of perpetrators and all crime organisations is a desire for profit and an intention to make criminal activities a source of regular income. An important role of denial of unlawful benefits can be seen during operations of law enforcement agencies aimed at combating cross-border organised crime as they hit the multi-aspect foundations of crime groups. Clearly, the main motivation driving perpetrators of criminal acts is the opportunity to gain regular economic benefits. It becomes a way of life. The more profitable it is, the stronger the motivation is to join organised crime groups. Financial

independence and quick profits are inherent elements of the success not only in legitimate economy but also in the grey zone, where assets can give the feeling of security and power[1].

Law enforcement agencies are trying to improve their criminal procedural and operational and exploratory activities to keep on par with the changing and evolving criminality. The constant search for ever new methods of concealing financial resources (benefits) forces institutions in charge of combating crime to implement even new legal measures and tactics to find and seize illegal assets.

The most recent initiative taken by law enforcement agencies aims at creating a legal environment for more effective denial of unlawful benefits by introducing new penal measures and improved acquisition of property-related information in cases conducted by law enforcement officers. The authors of the amendments to the criminal law and Acts on police services intended to prepare a set comprehensive legal norms aimed at disclosing unlawfully gained assets and benefits.

The legislative work resulted in amendments to the Code of Criminal Procedure, Criminal Code and the Police Act, which entered into force on 27 April 2017 under the Act of 23 March 2017 on amending the Act of the Code of Criminal Procedure and certain other Acts (Journal of Laws 2017, Item 768). The legislator introduced a new measure, broadly understood as „extended confiscation", to the Polish legal system. The concept includes a set of completely new or amended legal measures in the criminal code and the code of criminal procedure regarding property and seizure of assets for future court decisions.

The term „confiscation" is not expressed directly as a penal measure and there is no legal definition of confiscation in the current legal system. The legislative changes in question provide for adjudicating a penal measure (or rather a legal measure now) to meet one of the main objectives of criminal proceedings in the form of forfeiture of a business – a new solution in restitution of crime. In addition to the compensatory or remedial character, it has a preventive character as well. It serves the purpose of withdrawing a company, whether or not owned by the perpetrator, which was used for committing a crime or concealing benefits from that crime. Such potential forfeiture of a company is also a deterrent for any intentions of using a prosperous company in a criminal practice. The main reasons for adjudicating the aforementioned measure in criminal proceedings is gathering data or evidence which shows that a specific company was used for committing a crime or conceal benefits from a crime – regardless of whether it was established specifically for the purpose of criminal activity or used for such a purpose during legal operations. On this occasion, it is important to emphasise the role of economic entities established for the purpose of „VAT carousel fraud" or money laundering. If the company does not exist, is concealed or otherwise impossible to be forfeited, the law provides for adjudicating the measure with respect to other property of equivalent value. The same applies to the assessment of the origin of benefits – it is not required that a benefit is a direct unlawful income, it is sufficient if the perpetrator obtained it through conversion of financial resources or benefiting from crime. The legislator set the

[1] Own research – P. Trzciński; *Funkcja Scentralizowanego Pionu Policji w pozbawianiu sprawców korzyści finansowych z przestępczości zorganizowanej* [in:] *Wspólny Rynek nie tylko dla przestępców – SP Katowice 2011.*

threshold for forfeiture. A benefit, even indirect one, obtained by a perpetrator of a crime specified in the criminal code should amount to at least PLN 200,000 – in line with the definition of „assets of significant value"[2]. As for fiscal offences, this applies to benefits arising from large shortfalls in liabilities to the State Treasury i.e. around PLN 1,000,000[3]. Another premise to adjudicate forfeiture when a company is not owned by the perpetrator but a third party is a demonstrated will of that third party to have their company used for the purpose of committing a specific crime or concealing benefits from that crime or if that third party could foresee such a possibility and agreed to it. It does not have to be demonstrated if the company is owned by the perpetrator. The restriction of applicability of the measure to companies with a clearly identified owner, a natural person, may become a serious hindrance in practical application of the measure in question. The legislator provided for applying the provisions on forfeiture only to a company owned by a natural person, which seems problematic when one realises that majority of businesses involved in criminal activities are commercial law companies such as limited liability or listed companies, which have their own legal personality. By derogation, the legislator foresaw situations in which the procedural body may resign from securing specific assets and the Court may resign from adjudicating forfeiture of the company. Such situations include premises, demonstrated in the evidence proceedings, that are objectively dictated by social policies and guarantee protection against excessive legal repressiveness – like disproportionate situations i.e. the relation of the gravity of the crime and the degree of the defendant's fault or motivation to the behaviour of the owner of the company. Generally, the owner's failure to comply with the principles of diligence is the decisive factor here. The owner of a company threatened by forfeiture has the rights of a party with respect to procedural activities regarding that measure[4]. Similarly, disproportionality of the damage to the forfeiture also excludes application of the measure in question. If damage caused by a given crime or the value of a concealed benefit is not significant compared to the volume of the company's business, forfeiture is not adjudicated. This is an understandable derogation, as application of such a radical legal measure can lead to much more serious consequences that the amount of the damage caused by the perpetrator. Courts may also derogate from forfeiture in particularly justified cases where forfeiture of a company would be disproportionately painful to the owner. Such derogation is optional and depends of the assessment of evidence gathered in the case and data regarding property and family relations of the defendant. In the event of the aforementioned negative premises, the legislator ensured satisfaction of the main purposes of criminal proceedings[5] by creating an additional legal norm in Article 47 of the Criminal Code. In accordance with the new rule[6] that determines

[2] Article 115 Paragraph 5 – The Act on the Criminal Code, Journal of Laws 1997, No. 88, Item 553.

[3] Article 53 Section 15 – The Act on the Penal and Fiscal Code, Journal of Laws 1999, No. 83, Item 930 – *A significant value means value that exceeds the amount of 500 minimum salaries at the time of committing the prohibited act.*

[4] Article 91b of the Act on the Code of Criminal Procedure.

[5] *The provisions of the Code of Criminal Procedure are aimed at shaping criminal proceedings to take due account of the legally protected interests of the victim by a proportionate application of measures provided for n the criminal law.* – Article 2 of the Code of Criminal Procedure, Journal of Laws 1997, No. 89, Item 555, as amended.

[6] Article 47 Paragraph 2a of the Act on the Criminal Code (entry into force on 27 April 2017).

penal measures, the court may adjudicate punitive damages of up to PLN 1,000,000 for the benefit of the injured party or the Victims and Postpenitentiary Assistance Fund.

Another solution that belongs to the group of regulations referred to as „extended confiscation" is the right to adjudicate forfeiture of property gains, even indirect ones, in cases of alleged unlawful origins of those gains throughout a period for challenging the legality of such benefits extended to 5 years prior to the date of committing the first criminal act. The currently applicable provisions of law include a penal measure in the form of forfeiture of unlawful benefits, event indirectly unlawful ones. The prosecution and court practice shows that perpetrators tried to prevent the procedural organ from asserting claims regarding unlawful benefits. There may ways to convert such benefits, transfer property rights onto other persons or use them in other manners without committing acts bearing characteristics of money laundering. The investigator practice has given strong grounds to claim that in many cases of criminal proceedings, particularly initiated with respect to crimes discovered many years after they were committed, the legitimacy of the perpetrator's assets could not be verified beyond all doubt. This problem was observed mainly in the case of organised crime where perpetrators had made their crimes and affinity to criminal groups a regular source of income. To counter it, the legislator introduced into the criminal law system a derogation from the fundamental principle of the presumption of innocence where the burden of proving the defendant's guilt is on the procedural body and the defendant is not obliged to provide evidence of his or her guilt. The principle of the so-called „reversed burden of proof", which consist in an imperative presumption that property accumulated and owned by the perpetrator during the period since the first crime of significant value[7] represents unlawful benefit, has become the main weapon in combating organised crime[8]. Expansion of this presumption by a charge of ostensibility of the transfer of the property onto other person or entity prevents perpetrators from protecting their unlawful gains from criminal acts against seizure for the purpose of forfeiture. The set of amendments to the regulations regarding forfeiture of unlawful benefits made significant changes that provide for expanding the right to adjudicating forfeiture over time both with respect to the date of accumulating the property and types of crimes. Since the entry of the amendments to the Act[9] into force, it has been possible to use the presumption of criminal origin of specific benefits if the crime that brought those benefits is penalised by deprivation of liberty for at least 5 years or if the crime was committed in an organised crime group. In this light, a low enforcement agency may search for seizable property gained as long as 5 years before the crime up to the date of an applicable non-final sentence. The perpetrator or another interested person must supply evidence that is contrary to the presumption. The proof should demonstrate beyond any doubt that the identified property of the perpetrator comes from legitimate sources. If the title to the property is transferred onto any other person under any pretence, as is most

[7] See footnote 2.

[8] Article 45 Paragraphs 1-3 of the Criminal Code.

[9] The Act of 23 March 2017 on amending the Act on the Criminal Code and certain other Acts (entered into force on 27 April 2017).

often the case with crime groups, it is presumed that assets held by such other person in fact belong to the perpetrator unless that person could not, when acquiring them, presume that they could come from crime.

The provisions of the Code of Criminal Procedure now include the right to demand that a legal entity should return benefits obtained as a result of criminal acts committed by a person acting on its behalf[10]. In accordance with the law, the legal entity in question may be a representative or an officer of a corporate management body, who is then interviewed as a witness in criminal proceedings. Following a request by the prosecutor, the court may apply the provisions of the Civil Code and oblige such person or legal entity to return a specific gain or its equivalent to the authorised entity or adjudicate forfeiture of the gain or its equivalent for the benefit of the State Treasury. This solution is similar to one contained in the Penal Fiscal Code[11] which provides for asserting return of a benefit located in a commercial law entity or another entity specified in separate regulations.

In addition, the legislator clarified the provisions of the Code regarding the right to adjudicate forfeiture of unlawful benefits also in the case of the perpetrator's death, suspension or discontinuance of the proceedings or if the perpetrator absconds. It is a new solution in the Polish criminal procedure which now provides for adjudicating forfeiture without the conviction. Having regard to further aspects of handling seized unlawful benefits, which can now be used for satisfying equalisation claims raised by the victim, it is step in the correct direction, as it makes it possible to meet the postulate or restitution of the crime in by ensuring the victim's interests[12].

Amendments were also made to the provisions on establishing security on assets with respect to future property penalties as well as criminal measures regarding property and compensatory measures. The legal norm that regulates the grounds for establishing security on assets held by the defendant or suspect has now a catalogue of available legal measures. Point 5 of this catalogue deserves special attention[13]. Added as a legal measure we a point that reads „return to the victim or another authorised entity of a benefit, or an equivalent thereof, which the perpetrator gained from the crime committed". This is a legal measure that somewhat serves the purpose of securing a portion of the perpetrator's unlawful benefits for compensating losses incurred by the authorised entity, most often the victim. Of course, the legislator added a provision regarding the right to establish security on property of the entity obliged to return such benefit[14].

The aforementioned Act introduced a number of changes to Acts on activities conducted by State services in charge of detection and prosecution of crimes. The most important of those changes include the amendment to the provisions on operational and exploratory activities aimed at disclosing property subject to forfeiture. The provisions regulating operational

[10] The Penal Fiscal Code was expanded by adding a new Chapter 10a – The Obliged Entity.

[11] Article 24 of the Act on the Penal Fiscal Code, Journal of Laws 2007, No. 111, as amended.

[12] See footnote 4.

[13] Article 291 paragraphs 1 and 2 of the amended Act – the Act of 23 March 2017 on amending the Criminal Code and certain other Acts.

[14] More information – see footnote 10.

control by law enforcement agencies received an additional factual premise for such control also in the case of making findings regarding assets[15]. In accordance with the content of the added point regarding factual grounds for using operational control, such control may be used if respective activities are aimed at identifying property subject to forfeiture due to crimes referred to in Points 1-8 of Article 19 Paragraph 1 of the Police Act (i.e. in the case of serious crimes). Such operational activities are not restricted only to statutory methods of operational work involving telephone and premises tapping, but they include all legally permitted actions that fall within the statutory definition of the „operational control". However, the legislator went even further with the right to use operational control regarding identification of property. Of course, it restricted it only to seizable property, but at the same time added the right to use such control also for crimes listed in Article 45§2 of the Criminal Code and Article 33§2 of the Penal Fiscal Code. This gave law enforcement agencies the right to use methods of operational work individually, without the restriction arising from the catalogue of crimes in Article 19 Paragraph 1 Points 1-8 of the Police Act[16], and, importantly, expanded the right to use such methods in cases regarding crimes penalised by deprivation of liberty for at least 5 years and crimes where the perpetrator gained significant benefits. It becomes obvious here that the legislator gave law enforcement agencies the right to use advanced methods of operational work to a much wider extent in the case of identification of property than in the case of detection of perpetrators and preservation of evidence.

Significant changes were introduced in the provisions on the rights of respective services to acquire property-related information protected by professional privileges or other Acts[17]. In addition to acquisition of information from bank and insurance agreements, the Act now features a new catalogue of data held by such institutions as tax offices, general insurance companies, institutions running brokerage firms and financial instrument market institutions. The Police Act, which received the widest reaching amendments in this respect, features new legal solutions that facilitate exchange of information through electronic data exchange systems with and without a judicial review. An officer who conducts operational and exploratory activities is now able to quickly reach information on assets located by suspects or subjects of investigations. The key criterion differentiating acquisition of information from financial institutions and other offices or entity is the scope of information provided in a procedure with and without judicial review. By resigning from the long formal route of judicial review for the benefit of fast acquisition of information only under requests from authorised heads of respective organisational units, the legislator intentionally restricted the scope of data that can be obtained by an officer in such a manner[18]. It includes data excluding the most sensitive information from the perspective of the interest of its holder or data subject to important protection under specific Acts. In the author's opinion, it is a good solution that

[15] Article 19 Paragraph 1 Point 9 of the amended Police Act, Journal of Laws 1990, No. 30, Item 179, as amended.

[16] Although the author gives the provisions of the Police Act as an example, but the changes apply also to the Act on the Border Guard and other services.

[17] Article 20 of the amended Police Act (Form 1186, the text finalised upon considerations of amendments submitted by the Senate).

[18] Article 20 paragraph 5b of the amended Act.

serves the purpose of identifying where a perpetrator or person under operational control (due to a crime) may be locating unlawful gains if failure to act quickly prevents their identification and recovery. This solution is also very useful in combating tax crimes, particularly committed in an organised manner with the use of entities pretending legal business operations like e.g. „VAT carousels".

The aforementioned amendments to the criminal law and other Acts regarding disclosure, recovery and seizure of assets subject to forfeiture will significantly improve and accelerate the detective processes within law enforcement agencies and provide for faster implementation of the primary postulate of the Polish procedural criminal law regarding restitution of the crime and procedural guarantees for the victim.

Betina Tynka, Tomasz Zaborowski
ProCertiv Sp. z o.o.

Informatyka śledcza w zwalczaniu przestępstw korupcyjnych i gospodarczych

Streszczenie

Zarówno banki, jak i inne firmy oraz osoby, mogą paść ofiarą przestępstw finansowych, które stanowią istotny oraz stały element przestępczości związanej z obrotem gospodarczym. Aby radzić sobie z problemem przestępczości gospodarczej, organy ścigania oraz korporacje, powinny dysponować dużym zasobem informacji i nowoczesnymi narzędziami do wykrywania i zwalczania takich przestępstw.
W tym celu konieczne jest zastosowanie metod informatyki śledczej, z uwzględnieniem referencyjnego modelu postępowania z dowodami elektronicznymi (EDRM). Opiera się on na właściwym zabezpieczeniu i akwizycji danych z nośników cyfrowych oraz chmury, przetworzeniu i segregacji danych oraz ich analizie. Etap łącznej analizy wielu różnych danych, pochodzących
z różnych źródeł jest kluczowy w sprawach gospodarczych i dotyczących przestępczości zorganizowanej.
Istnieją narzędzia informatyki śledczej, takie jak platforma analityczna Nuix, które pozwalają na pełną analizę artefaktów komunikacyjnych, wyszukiwanie powiązań pomiędzy osobami, firmami, badanie dokumentów wraz z porównywaniem ich zawartości i wyświetlaniem różnic w ich treści. Znajomość nowych trendów i rozwiązań w informatyce śledczej jest kluczem do zwalczania przestępstw korupcyjnych i gospodarczych.

Jako zespół specjalistów zajmujących się informatyką śledczą od 14 lat, opracowaliśmy autorską metodykę zabezpieczania i analizy danych. Specjalizujemy się w sprawach gospodarczych wymagających zastosowania zaawansowanych narzędzi i wiedzy, którą dzielimy się podczas licznych szkoleń, zarówno dla organów ścigania, jak i osób prywatnych.

Charakterystyka danych zawierających informacje o przestępstwach gospodarczych

W obecnych czasach korzystanie z rozwiązań informatycznych jest nieodzownym elementem prowadzenia firmy, przedsiębiorstwa lub innej formy biznesu. Funkcjonowanie firmy opiera się w dużej mierze na korzystaniu z technologii IT, począwszy od infrastruktury technicznej, czyli komputerów, serwerów i dostępu do Internetu, po korzystanie z oprogramowania i specjalistycznych narzędzi. Powszechna grupa programów, w których powstają cenne z punktu widzenia śledczego dane, to systemy operacyjne, pakiety biurowe, programy finansowo-księgowe, programy CRM, platformy ERP.

Obszary, w których powstają dane zawierające informacje o potencjalnych przestępstwach gospodarczych to księgi rachunkowe, umowy, oferty, a także elektroniczna komunikacja wewnętrzna i zewnętrzna. Wielkość przedsiębiorstwa definiuje jak zaawansowane rozwiązania informatyczne są wykorzystywane i jaka ilość danych jest przetwarzana w danej firmie. Współczesne rozwiązania pozwalają na redukcję kosztów infrastruktury IT i obsługi informatycznej, poprzez wynajem przestrzeni dyskowej wraz z oprogramowaniem w tzw. chmurze. Zwalnia to przedsiębiorców z utrzymywania drogich działów IT oraz redukuje nakłady finansowe na bezpieczeństwo danych.

Kolejnym ważnym aspektem w kontekście przestępstw gospodarczych jest korzystanie z urządzeń mobilnych, głównie smartfonów i tabletów. Należy tutaj zwrócić uwagę, że coraz popularniejsze jest korzystanie z telefonii VOIP oraz komunikatorów internetowych typu Messenger, WhatsApp, FaceTime, Signal itd., także w celach biznesowych. W związku z tym konieczne jest pochylenie się nad danymi pochodzącymi z urządzeń mobilnych i aplikacji.

Jednak to, co dla przedsiębiorców jest optymalnym rozwiązaniem biznesowym, staje się problemem dla organów kontroli, ścigania czy sądów. Istotą problemu jest fakt, że rozwiązania informatyczne nie idą w parze ze stanowionym prawem, które pozwalałoby na skuteczne wyegzekwowanie dostępu do informacji finansowej, dokumentów czy zapisów komunikacji. Kolejnym problemem jest prawne uregulowanie kwestii zabezpieczania danych znajdujących się poza nośnikiem, np. komputerem, czyli w „chmurze".

Typy danych, które wykorzystuje się do wykazania przestępstwa gospodarczego

Na przestrzeni ostatnich lat zaobserwowano, że głównym źródłem danych w przestępstwach gospodarczych są zapisy finansowo-księgowe, które gromadzone są w bazach danych tj. MS SQL, ORACLE, MY SQL, SYBASE itd. Należy podkreślić, że miejsce powstawania faktur może być inne niż prowadzenie ksiąg rachunkowych. Kolejny istotny typ danych to dokument zawierający zestawienia tabelaryczne, umowy, oferty handlowe, zamówienia, raporty, faktury, dokumenty magazynowe itd. Do tej grupy należy także zaliczyć pliki graficzne zawierające obrazy dokumentów powstałych w procesie digitalizacji oraz zdjęcia. Występują one najczęściej w formatach pdf, jpeg, tiff. Dane typu „dokument" powstają w programach biurowych tj. Microsoft Office, OpenOffice, LibreOffice itd. i zazwyczaj są to pliki w formatach doc, docx, xls, xlsx, pdf, txt.

Nieodzownym elementem biznesu jest wymiana informacji. Podstawową formą komunikacji jest e-mail i nic nie wskazuje, żeby w najbliższej przyszłości miało się to zmienić. Dodatkowo coraz powszechniejsze stają się komunikatory do przesyłania wiadomości głosowych, tekstowych oraz plików.

Kolejnym źródłem, z którego mogą być pozyskiwane informacje, są źródła zewnętrzne tj. wyciągi bankowe, bilingi telefoniczne, protokoły przesłuchań, dane internetowe, dokumenty w formie papierowej.

Sposoby pozyskiwania cyfrowych danych dowodowych

Model zabezpieczenia stosowany jeszcze nie tak dawno, polegający na zabezpieczaniu całych jednostek komputerowych lub wykonywaniu kopii binarnych, jest modelem przestarzałym.

W jego wyniku gromadzi się bardzo duże ilości danych, z których około 70% jest nieprzydatnych pod kątem uzyskania pożądanej informacji. Ponadto taka forma zabezpieczenia paraliżuje działalność firmy, a ogromne ilości danych, które są przetwarzane, utrudniają proces wykrywczy.

Nowy model zabezpieczania polega na zabezpieczaniu wyselekcjonowanych typów danych charakterystycznych dla biznesu, przez co sam proces jest szybki i niweluje pobieranie niepotrzebnych danych. W sprawach gospodarczych najczęściej zabezpiecza się bazy danych, wiadomości e-mail, dokumenty w różnych formatach, w tym pdf, oraz pliki graficzne. Dane te przechowuje się zarówno na nośnikach fizycznych, takich jak smartfon, notebook, desktop, serwer, jak i na wirtualnych dyskach i w „chmurach". Wirtualizacja platform biznesowych powoduje, że coraz chętniej grupy przestępcze korzystają z tej formy prowadzenia biznesu.

Obecnie stosowane techniki akwizycji danych to kopia smartfona, tworzenie kontenerów z wyselekcjonowanych grup danych, np. dokumentów, e-maili oraz akwizycja celowa przy wykorzystaniu „skanerów", czyli programów do wybiórczego zabezpieczania danych. W tym celu stosuje się specjalistyczne oprogramowanie typu Nuix Collector, które umożliwia zabezpieczanie konkretnych, wcześniej zdefiniowanych danych w formie kontenerów. Z kolei w przypadku danych wirtualnych, takich jak skrzynki mailowe znajdujące się na serwerach zewnętrznych, np. Gmail, konta Dropbox, Google Drive, Microsoft OneDrive, Box, Apple iCloud, SharePoint Server, Amazon S3 Buckets, MS SQL Server, SSH Server, Documentum Server, stosuje się narzędzie Nuix Imager.

Model badań kryminalistycznych polegający na syntezie i analizie danych pochodzących z wielu źródeł dowodowych

W trakcie procesu przygotowawczego zostają zgromadzone dane z wielu źródeł dowodowych, które przed przystąpieniem do analiz należy odpowiednio przygotować. Proces ten należy podzielić na dwa etapy. Pierwszy etap to przygotowanie danych polegające na zamianie dokumentów z formy papierowej na cyfrową, odzyskanie danych, selekcja i segregacja danych, redukcja powtarzających się danych, odrzucenie danych niezawierających informacji (dane systemowe, szablony dokumentów, puste formularze i foldery, spam itp.), uproszczenie danych zawartych w zbiorach archiwum, wydzielenie danych z baz danych.

Wyselekcjonowane i uproszczone dane należy poddać drugiemu etapowi - analizie w jak najmniejszej ilości programów analitycznych, które pozwalają pracować na maksymalnej liczbie źródeł. Najlepszym rozwiązaniem jest zastosowanie programów klasy eDiscovery. Z naszej praktyki wynika, że doskonale w tej roli sprawdza się Nuix Investigator, który jest programem analitycznym przystosowanym do pracy na ogromnych ilościach danych różnych typów. Pozwala on między innymi na wyszukiwanie powiązań w plikach pochodzących z różnych źródeł, wskazywanie plików takich samych i podobnych, zaznaczanie różnic w treści dokumentów oraz automatyczne wyszukiwanie wyrażeń regularnych, co jest szczególnie przydatne w analizie spraw gospodarczych. Tym sposobem można wskazywać nazwy osób i podmiotów, sumy pieniędzy, numery kont, NIP, PESEL i wiele innych. Nuix Investigator jest także przystosowany do analizy komunikacji, zarówno mailowej, jak i telefonicznej i przez aplikacje.

Odmienną kwestią jest analiza danych finansowo-księgowych, gdzie dane są w formie papierowej i cyfrowej, co dodatkowo wymaga analizy przez biegłych rewidentów, a czas analizy liczony jest w tygodniach.

Dokumentowanie i prezentowanie przebiegu przestępstwa w informatyce śledczej

Kluczową kwestią w przedstawianiu wyników analiz jest przejrzysty system raportowania. Forma raportu jest zależna od celów badania oraz materiału dowodowego, który został przekazany do analizy. W przypadku pojedynczych urządzeń mobilnych generowany jest interaktywny raport, który zawiera wszystkie dane pozyskane z urządzenia, także dane usunięte. Interaktywność raportu polega na możliwości samodzielnego wyszukiwania przez śledczego konkretnych informacji, co pozwala na szybkie i celne pozyskiwanie dowodów. Z kolei, wynikiem złożonych analiz jest grupa raportów, zarówno tekstowych, jak i graficznych, które są generowane według jednego szablonu. Jest to ważna kwestia z punktu widzenia standaryzacji pracy i zachowania jednolitości opinii. Raporty generowane są najczęściej w formatach pdf, html, csv, txt, svg, png, w zależności od ilości danych eksportowanych i ich typu, a także formatów, w których dany program umożliwia raportowanie.

Ze względu na ilość treści, którą niesie raport w obecnych czasach, jest on zapisywany na nośniku elektronicznym, który dołączany jest do sprawozdania z badań. Samo sprawozdanie z badań wraz z opinią wydawane jest w formie papierowej i zawiera wszystkie niezbędne treści, tj. założenia badawcze, opis metody badawczej, część badawczą, opinię, raport techniczny oraz instrukcję odczytu raportu dołączonego w formie elektronicznej na nośniku. Taki sposób raportowania z jednej strony jest konieczny, ze względu na obszerność materiału dowodowego, a z drugiej jest przejrzysty i wygodny dla osoby, która taką opinię otrzymuje.

Betina Tynka, Tomasz Zaborowski
ProCertiv Sp. z o.o.

Computer forensics in combating corruption and economic crime

Abstract

Banks, companies and private individuals alike may fall victim to financial crimes - a major and permanent element of economic criminality. In order to handle the problem, corporations and law enforcement agencies need a large resource of information and modern tools designed to detect and combat such crimes. To this end, it is necessary to employ methods of computer forensics, including the Electronic Discovery Reference Model (EDRM). The model is based on appropriate securing, acquisition, processing, segregation and analysis of data from a cloud and digital storage media. The phase of aggregated analysis of multiple pieces of information from various sources is essential in cases related to economic and organised crime.

There are computer forensics tools, such as the Nuix analytical platform, which provide for a complete analysis of communications artefacts, search of connections between individuals and companies and examination of documents including comparing them and displaying differences in their content. The knowledge of new trends and solutions in computer forensics is the key to combating corruption and economic crime.

As a team of experts with 14 years of experience in computer forensics, we have developed an original methodology for securing and analysing data. We are specialised in economic cases that require application of advanced tools and knowledge, which we share with others during numerous training courses for law enforcement agencies and private individuals.

Characteristics of data containing economic crime information

In this modern day and age, application of computer solutions is an essential element of running a company, an undertaking or other forms of business. Business operations rely largely on IT technologies ranging from technical infrastructure – i.e. computers, servers and Internet access – to computer software and specialist tools. A group of widely used computer programmes wherein data valuable to investigators is produced includes operating systems, office packages, financial and accounting software, CRM software and ERP platforms.

Areas where data with potential economic crime information is created include accounting books, agreements, offers as well as electronic communication, both internal and external. How advanced are specific IT solutions employed and what amount of data is processed in a specific company depend on the size of that company. Modern solutions provide for reducing IT infrastructure and support costs by means of rental of disc space with software

in the so-called cloud. It relieves businesses from the necessity to maintain expensive IT departments and reduces financial expenditures on data security.

Use of mobile devices, mainly smartphones and tablets, is yet another important aspect in the context of economic crime. Indeed, it must be noted here that with the growing popularity of VoIP telephony and Internet messengers like WhatsApp, Messenger, FaceTime, Signal, etc. for business purposes, one must look more closely at data generated in mobile devices and applications.

However, what is an optimum solution for businesses becomes a problem for control and law enforcement authorities and courts. The core of the problem is that IT solutions do not go hand-in-hand with the written law, which, if they did, would provide for efficient enforcement of access to financial information, documents and communication records. Regulation of the issue of securing data which is stored externally, i.e. in the cloud, is another problem.

Types of data used for demonstrating an economic crime

Financial and accounting records stored in databases like MS SQL, ORACLE, MY SQL, SYBASE, etc. could be observed as the main source of information on economic crime over the recent years. It must be emphasised that the place where invoices are created may not be the same as the place where accounting books are kept. Documents with tabulated data, agreements, commercial offers, orders, reports, invoices, warehouse documents, etc. represent another important type of data. This group includes also graphic files – most often in pdf, jpeg and tiff formats – with photographs and images of documents created in the process of digitisation. „Document"-type data is created in office programmes i.e. Microsoft Office, OpenOffice, LibreOffice, etc. and is usually saved in doc, docx, xls, xlsx, pdf, txt files.

Exchange of information is essential in business. E-mail is the primary form of communication and nothing indicates this will change in the nearest future. In addition, messengers for sending voice and text messages and files are becoming more and more popular.

Information can also be acquired from also external sources i.e. bank statements, phone bills, interview records, Internet data, and paper documents.

Methods of acquiring digital evidence

The recent model of securing evidence which consists in securing entire computer units or making binary copies is obsolete now. It leads to gathering large volumes of data of which some 70% is useless for finding a specific desired piece of information. It also paralyses business operations and the enormous volumes of data to be processed impede the detective process.

The new model involves securing selected types of business-specific data, which makes the process fast and eliminates gathering unwanted data. Evidence secured in economic cases most often includes databases, emails, graphic files and documents in various formats, including pdf. The data is stored on physical media, such as smartphones, notebooks, desktop computers and servers, as well as virtual discs and „clouds". Virtualisation of business platforms is making these forms of business activities increasingly popular among crime groups.

Data acquisition methods in use today include making smartphone copies, creating containers of selected groups of data, e.g. documents and emails, and focused acquisition

by means of „scanners" i.e. programmes for securing data in a selective manner. This is done by specialist software like Nuix Collector, which provides for securing specific pre-defined data in the form of containers. As for virtual data – such as mailboxes on external servers like e.g. Gmail, Dropbox, Google Drive, Microsoft OneDrive, Box, Apple iCloud, SharePoint Server, Amazon S3 Buckets, MS SQL Server, SSH Server and Documentum Server – the Nuix Imager tool is used.

Forensic examination model based on synthesis and analysis of data from multiple evidence sources

Data from multiple evidence sources is gathered during the preparatory process and it must be sufficiently prepared before commencing analyses. This process should be divided into two phases. The first phase involves transforming the documents from the paper into electronic form, retrieving the data, selecting and segregating the data, reducing duplicated data, rejecting data that carries not information (system data, document templates, empty forms and folders, spam etc.), simplifying archived data and extracting data from databases.

The selected and simplified data must then undergo the second phase – analysis by means of the least possible number of analytical programmes that provide for working on the maximum number of sources. eDiscovery class of software is the best solution here. Our practice shows that Nuix Investigator is excellent for the purpose. An analytical programme designed to work on huge volumes of various data, it provides for, among others, searching for links in files from different sources, detecting identical and similar files, marking differences in the content of documents and automatic search for regular phrases, which is particularly useful in analysing economic cases. This way, investigators can identify names of individuals and entities, sums of money, numbers of accounts, tax and personal ID numbers (NIP/PESEL) and many more. Nuix Investigator can also analyse communication, whether it is email, telephone or application based.

A separate area is analysis of financial and accounting data, normally stored in paper and digital form, which requires an additional analysis by expert auditors and takes weeks to complete.

Documenting and presenting the course of a crime in computer forensics

A clear reporting system is of key importance for presenting findings. The form of a specific report depends on the objectives of the investigation and evidence submitted for analysis. In the case of individual mobile devices, an interactive report is generated which contains all data acquired from the device, including deleted data. The interactive functionality of the report allows the investigator to independently search for specific information, thus providing for fast and accurate acquisition of evidence. On the other hand, complex analyses produce a group of reports, both text and graphic, which are generated according to a single template. This is important for standardisation of the work and unity of the opinion. Reports are normally generated in pdf, html, csv, txt, svg and png formats, depending of the type and volume of data exported and reporting formats offered by specific software employed.

Due to the volume of content carried by such a report nowadays, it is normally saved on an electronic media which is attached to the overall examination report. The examination report and opinion are produced in paper form and include all necessary information i.e. examination assumptions, a description of the examination method, the examination part, the opinion, a technical report and manual for reading the attached electronic report. This manner of reporting is, on the one hand, necessary because of the volume of evidence gathered and, on the other, clear and reliable for the addressee.

Krzysztof Mendyk
Izba Administracji Skarbowej w Opolu, Opolski Urząd Celno-Skarbowy

Transfery pieniężne z krajów UE do krajów Dalekiego Wschodu niemające odzwierciedlenia w transakcjach gospodarczych

Streszczenie

Prezentacja dotyczy dość często spotykanego problemu transferów dużych kwot z kont firm i osób fizycznych z terytorium jednego z krajów unijnych z Zachodniej Europy na konta firm zarejestrowanych przez obywateli zagranicznych na terenie Polski. Kolejnym etapem przepływu środków jest ich transfer do Chin, na konta bankowe firm oraz osób fizycznych. Firmy prowadzące działalność i zarejestrowane w Polsce nie prowadzą żadnej działalności gospodarczej,z kolei dostęp do danych osób i firm w Chinach jest mocno utrudniony. Głównym założeniem śledczych prowadzących tego rodzaju sprawę było udowodnienie prania pieniędzy oraz możliwości finansowania terroryzmu. Postępowanie w tej sprawie znajduje się obecnie na etapie prokuratorskim.

Z czym kojarzy nam się daleki Wschód, Chiny, Hongkong, Singapur?

Z pewnością każdy powie, że z rozwiniętą siecią usług finansowych, tanią siła roboczą, produktami dziewiarskimi, zabawkami, tudzież innymi artykułami w niskich cenach sprowadzanymi masowo na teren Unii Europejskiej.

Ale czy może nam się kojarzyć z finansowaniem terroryzmu i nielegalnym obrotem gospodarczym?

To nie jest już takie oczywiste, a jednak ma miejsce.

Terroryzm to nie tylko ISIS i wojna na Bliskim Wschodzie, to również działania osób i państw zmierzające do destabilizowania gospodarek krajów rozwijających się. To także zasilanie w środki finansowe grup ekstremistycznych w Europie i powodowanie powszechnego strachu w społeczeństwie.

Jednakże nie byłoby to możliwe bez pieniędzy. Pieniędzy wprowadzanych do systemu gospodarczego pod pozorem legalnych transakcji.

Służby skarbowe, a także obecnie Krajowa Administracja Skarbowa (KAS) dążyły i dążą obecnie do wykrywania transakcji finansowych, które pozornie noszą cechy naturalnych przepływów finansowych pomiędzy przedsiębiorcami, a w rzeczywistości służą do finansowania przedsięwzięć nielegalnych, np. terroryzmu, a także wskazują na możliwość

zaistnienia procederu przestępczego noszącego potoczną, choć już utrwaloną w literaturze nazwę „prania pieniędzy".

Uzyskanie wiedzy na temat tego typu transakcji wymaga od funkcjonariuszy KAS dużej wiedzy, praktyki oraz wykorzystywania narzędzi tak nowych jak i tradycyjnych. Jako *novum* można uznać szerokie stosowanie analizy kryminalnej i związanej z nią prawidłowej interpretacji wniosków. Jednakże nie należy zapominać o tradycyjnych formach zdobywania informacji jakimi są: praca z osobowymi źródłami informacji, wywiad czy też łączenie i wieloźródłowe weryfikowanie uzyskanych informacji, bowiem nawet najlepsza analiza może być obarczona błędem w postaci niewłaściwie przyjętego założenia czy też nieprawidłowego skonstruowania pytań i celu analizy.

Funkcjonariusze opolskiego KAS w toku prowadzonych czynności uzyskali potwierdzone i zweryfikowane kilkuźródłowo informacje o fakcie przepływów finansowych pomiędzy osobami fizycznymi zamieszkującymi terytorium Francji i Wielkiej Brytanii a firmami założonymi przez obywateli francuskich na terenie Polski.

Dalsza analiza zgromadzonego materiału pozwoliła na ustalenie, że:

- nadawcami przelewów były młode, niepracujące osoby posiadające obywatelstwo francuskie pochodzenia arabskiego,
- siedziby, adresy nadawców to były biura wynajmowane we Francji i Wielkiej Brytanii stanowiące odpowiednik polskich „wirtualnych biur",
- obywatele francuscy zakładający i prowadzący firmy w Polsce rejestrowali swoje podmioty również w wirtualnych biurach. Dla celów urzędowych w stosunku do organów francuskich podawali oni adresy polskie, gdzie byli zameldowani, ale nigdy tam nie zamieszkiwali, a w Polsce posługiwali się adresami francuskimi,
- pełnomocnictwa do prowadzenia spraw firm, ponieważ było ich kilka, były sporządzane we francuskich biurach notarialnych, z tym że pełnomocnicy, tak posiadający obywatelstwo polskie, jak i francuskie nie mieli świadomości ich uzyskania, jak i nie przebywali w Polsce i nie prowadzili żadnych czynności w imieniu firm,
- upoważnienia do dysponowania rachunkami bankowymi firm posiadało tylko dwóch głównych organizatorów procederu – obywateli francuskich – przebywających w Polsce.

Kolejnym krokiem podjętym przez funkcjonariuszy służb skarbowych było przeanalizowanie działalności gospodarczej jaką prowadzili francuscy przedsiębiorcy i okazało się, że część firm to tzw. uśpione, czyli nie deklarujące żadnych obrotów, a część deklarowała dla celów podatkowych niewielkie kwoty.

Posiadając informacje o możliwych znacznych wpływach na konta firm zwrócono się do Generalnego Inspektora Informacji Finansowej o udzielenie informacji o wpływach i wypływach środków pieniężnych z kont firm objętych zainteresowaniem.

Dopiero uzyskanie tych informacji dało całościowy obraz procederu przestępczego.

Firmy otrzymały w latach 2013-1015 środki w wysokości około 21 mln euro w różnych walutach, a następnie zarówno te środki, jak i pochodzące z nieustalonych wtedy źródeł przekazały na konta w Chinach i Hongkongu.

Transfery w tych samych latach na konta azjatyckie wyniosły około 40,5 mln euro oraz wypłacono gotówką na terenie Polski 160 tys. euro, co w naszym rozumieniu stanowiło zapłatę dla przedsiębiorców francuskich za usługę przetransferowania tak dużych środków.

Kolejne czynności podejmowane w ramach badania opisanego wyżej procederu polegały na próbie ustalenia właścicieli kont bankowych, na które były przelewane środki z kont firm zarejestrowanych w Polsce. W miarę możliwości ustalono, że część rachunków należy do osób fizycznych, a część do konsorcjów finansowych zajmujących się transakcjami na rynku finansowym.

Równolegle do prowadzonych czynności uzyskano informacje o zainteresowaniu służb francuskich działalnością ich obywateli na terenie RP. Pozwoliło to na nawiązanie współpracy, jednakże była ona mocno ograniczona, ale stała się przyczynkiem do wszczęcia czynności dochodzeniowych przez prokuraturę oraz powierzenia śledztwa Agencji Bezpieczeństwa Wewnętrznego.

Śledztwo z uwagi na zakres i stopień skomplikowania jest nadal w toku.

Ze strony służb skarbowych podjęto czynności zmierzające do objęcia kontrolami podatkowymi wszystkich firm objętych zainteresowaniem.

W trakcie czynności realizacyjnych zabezpieczono środki na kontach bankowych oraz gotówkę w domu jednego z francuskich przedsiębiorców, a także urządzenia elektroniczne, których zbadanie przez biegłych może pomóc w ustaleniu powiązań i możliwego ich udziału w finansowaniu terroryzmu.

Policja, organy bezpieczeństwa państwa i służby celno-skarbowe powinny ściśle współpracować w sprawach gospodarczych oraz związanych z popełnianiem przestępstw polegających na tzw. „praniu pieniędzy". Pozwala to na większą efektywność oraz szybsze zidentyfikowanie procederu przestępczego.

Istotne jest również zaangażowanie banków i świadomość bankowych służb bezpieczeństwa, że za pomocą prowadzonych w nich rachunków może dochodzić do nielegalnych transferów finansowych, co powinno przełożyć się na niezwłoczne informowanie o tym fakcie Generalnego Inspektora Informacji Finansowej.

Krzysztof Mendyk

Regional Revenue Administration Chamber in Opole, Customs and Tax Office in Opole

Money transfers from EU countries to Far Eastern countries that are not reflected in economic transactions

Abstract

The presentation concerns a quite common problem of transfers of large amounts from corporate and private bank accounts in an EU Member State in the Western Europe into bank accounts of companies registered by foreign nationals in Poland. The next step in the flow of funds is transfer into corporate and private bank accounts in China. The companies established and running business in Poland are in fact not running any business at all, while access to details of the individuals and companies in China is considerably difficult. The main objective of the investigators working the case concerned was to prove money laundering and possible financing of terrorism. The proceedings in the case are now at the prosecution level.

What do we associate with the Far East, China, Hong Kong, Singapore?

Everyone will surely say it is a well developed network of financial services, cheap labour force, textiles, toys or other low-price products imported in great numbers to the European Union.

But can it be terrorism financing and illegal trade?

Although not that obvious, it does take place.

Terrorism is more than just ISIS and the war in the Middle East. It encompasses actions taken by individuals and states to destabilise economies of developing countries. It also involves financing extremist groups in Europe and instilling widespread fear among the general public.

However, all this would not be possible without money - money which is introduced into the economic system under the guise of legal transactions.

Poland's tax revenue services, and now also the National Revenue Administration (Polish: Krajowa Administracja Skarbowa, KAS), are striving to detect financial transactions which are seemingly natural financial flows between businesses but which in fact serve to finance illegal undertakings, such as terrorism, and signal the possibility of the criminal practice which is commonly referred to, also in the professional literature, as money laundering.

Gaining knowledge on such transactions requires KAS officers to possess expertise, practical experience and ability to employ new as well as traditional tools. A wide application of crime

analysis and the related appropriate interpretation of findings can be regarded as a novelty in this field. However, one must not ignore traditional methods of information gathering such as work with personal sources of information, intelligence gathering and combining and multi-source verification of findings, for even the best of analyses may be flawed by wrong assumptions or inappropriately formulated questions or objectives.

KAS officers in the City of Opole operationally gained information, which was confirmed and verified by several sources, on financial transfers between private individuals residing in France and the United Kingdom and businesses established by French nationals in Poland.

A further analysis of the intelligence provided for establishing that:

- the transfers were sent by young unemployed French citizens of Arabic descent;
- the places of establishment and addresses of the senders were offices rented in France and the United Kingdom whose equivalents in Poland are referred to as "virtual offices";
- the French nationals who established and ran their businesses in Poland also used virtual offices for the purpose. For official purposes, when contacting French authorities, they would use their Polish addresses at which they were registered but never actually lived, while using their French addresses when operating in Poland;
- authorisations to handle business matters of the companies, because there were several companies involved, were notarised at notary offices in France, but the authorised representatives, both French and Polish nationals, were neither aware of their authorisations nor stayed in Poland nor performed any transactions on behalf of the companies;
- authorisations to operate the companies' bank accounts were held only by two main organisers of the ill-practice, both French nationals, who were staying in Poland.

Another step taken by the revenue service officers was to analyse the economic activity of the French undertakings. They found that some of the companies had been the so-called "sleeping" companies i.e. they either did not report any turnover or reported small amounts for tax purposes.

Equipped with information on possible sizeable inflows into the companies' accounts, the KAS requested the Inspector General of Financial Information to provide information on incoming and outgoing transfers on the accounts concerned.

Only with the requested information did the complete picture of the ill-practice become evident.

The companies received around Euro 21 million of funds in different currencies in 2013-1015, and subsequently transferred those funds, as well as other funds from then unidentified sources, into bank accounts in China and Hong Kong.

In the period concerned, the transfers into the Asian accounts amounted to Euro 40.5 and further Euro 160,000 was withdrawn in cash in Poland, which we understand was remuneration paid to the French undertakings for the service of transferring such large amounts.

Further actions taken as part of the investigation of the ill-practice in question involved efforts to establish the owners of the bank accounts into which the Polish-registered companies transferred the funds. It was established, to the extent permitted by the circumstances, that

some of the accounts were owned by private individuals while others by financial consortia conducting transactions on the financial market.

In parallel to the aforementioned actions, information was obtained regarding the French services' attention to activities of their citizens in the Republic of Poland. That provided for establishing cooperation which, albeit very limited, contributed to initiating investigative actions by the prosecution office and placing the investigation in the hands of the Internal Security Agency.

Due to its scope and complexity, the investigation is still in progress.

The tax revenue services moved to conduct tax audits in all companies concerned.

The enforcement activities have led to seizing of funds on the bank accounts and cash at home of one of the French entrepreneurs as well as electronic devices which, when analysed by experts, can help in establishing their links and possible involvement in terrorism financing.

There should be close cooperation between the Police, State security authorities and custom and revenue services in economic cases and cases related to the so-called "money laundering". This provides for better efficiency and faster identification of ill-practices.

Other important aspects include involvement of banks and awareness of bank security services that accounts kept in their banks may be used for illegal financial transfers, which, when detected, should be immediately reported to the Inspector General of Financial Information.

Jacek Baranowski

Financial Intelligence Group, EUROPOL

The role, and support of EUROPOL in financial investigations. Cooperation with Member States

Abstract

This paper discusses the scope of money laundering activities in the European Union countries. Technological innovations in communication systems accompanied by a wider use of cash-less financial transactions provide Transnational Organised Crime Groups with tools for planning and committing a range of crimes. The Financial Intelligence team (FI) within Europol supports Member States with intelligence and forensic support to prevent and combat international money laundering activities. The main goals of the team involve finding the criminals involved in money laundering, disrupting their associates and confiscation of the proceeds of their crimes.

A strong cooperation between Europol and the European Union countries resulted in successful outcomes such as seizing considerable amount of criminal assets.

Organized Crime Groups and Money Laundering

The money laundering activities currently detected and investigated by Law Enforcement Agencies in the European Union are characterized by a combination of convergent elements which make the Money Laundering phenomenon a perfect symbiosis between tradition and innovation. The large number of possibilities offered by the modern communication systems has provided Transnational Organised Crime Groups with a boundless platform over which criminal interests are planned, developed and consolidated. This has been accompanied by the development of the international banking sectors which is now moving toward a wider use of cash-less financial instruments where financial transactions can also be performed remotely.

Furthermore, new possibilities have been offered by the socio political developments of the European Union which formally integrates different States into a unique political system with a single market and large territories across European Union Countries where persons and goods are moving freely. The absence of internal European Union boundaries, the introduction of the Euro currency along with the new requirements coming from the implementation of the 3rd European Union Money Laundering Directive have pushed both European Union and non-European Union Organised Crime Groups to consistently increase the use of monetary instruments in order to inject/place criminal proceeds and avoid Law Enforcement detection. It is in the framework of this quite complex and peculiar scenario that the Money Laundering offence is committed today by European Union transnational

Organised Crime Groups regardless of their ethnic origin and/or geographical location of criminal networks involved.

Criminal Finances and Money Laundering

Money laundering allows Organised Crime Groups to introduce the proceeds of crime into the legitimate economy. Almost all criminal groups need to launder profits generated from criminal activities; however, the way in which money laundering is carried out varies greatly depending on an Organised Crime Group's level of expertise as well as the frequency and scale of money laundering activities.

Criminal networks continuously seek to exploit the latest technological developments such as cryptocurrencies and anonymous payment methods. Rapid transaction processing and the proliferation of effective anonymization tools are significant obstacles in the identification of the beneficial owners of criminal proceeds. A growing number of online platforms and applications offer new ways of transferring money and are not always regulated to the same degree as traditional financial service providers.

Money launderers heavily rely on document fraud to facilitate their activities. Fraudulent documents such as false invoices and forged ID documents are used to conceal the origin of criminal cash, to open bank accounts or to establish shell companies.

Money launderers provide services to both organised crime and terrorist organisations. The most common methods of money laundering are:

- Cash smuggling: by couriers or using post and parcel services. **Cash** remains at the core of the money laundering business. Cash continues to be smuggled by **couriers** and, increasingly, by **post** and **parcel services**.
- Money laundering syndicates, relying on a network of middlemen and complex laundering techniques. **Money laundering syndicates** offer complex laundering techniques and carry out the laundering operations on behalf of Organised Crime Groups in exchange for a commission of between 5% and 8%, these syndicates.
- Trade-based money laundering: false invoicing and forged ID documents are used by shell companies owned by Organised Crime Groups to conceal criminal funds. **Trade-based money laundering** is a highly effective way of concealing criminal funds by **manipulating or forging purchases or sales** using double invoicing, false invoicing by companies that are owned by Organised Crime Groups, associates and relatives.
- New payment methods such as cryptocurrencies and anonymous payment methods are significant obstacles in the identification of the beneficial owners of criminal proceeds. **New payment methods** such as cryptocurrencies, prepaid cards, online payment and internet vouchers are continuously emerging and are generally **less well-regulated than traditional payment methods**.

Legal actors appearing in Money Laundering schemes:

COMPANY SERVICE PROVIDERS

According to FATF report of 2010 on Money Laundering Using Trust and Company Service Providers (TCSPs) play a key role in the global economy as financial intermediaries, providing an important link between financial institutions and many of their customers. They provide often invaluable assistance to clients in the management of their financial affairs and can therefore significantly impact transactional flows through the financial system.

Corporate service providers (CSPs) are usually represented by lawyers and financial experts. Financial experts can be:

1) Entities that act as formation agent of legal persons, whose services include being (or arranging a third party to act as) a nominee shareholders for another person
2) Entities acting as (or arranging a third party to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons.
3) Entities providing a registered office, business address or accommodation, correspondence administrative address for a company, a partnership or any other legal person or arrangement.
4) Entities acting as (or arranging a third party to act as) a trustee of an express trust.

There is an important link between CSPs and offshore entities as most of the companies specialising in services indicated above are registered in offshores. This implies that:

1) All the administrative issues are figured out by the offshore company, for example well known from the Panama Papers – Mossack Fonseca. They not only help with the paperwork, but also help to choose the most suitable tax haven depending on the purpose of the client: the British Virgin Islands for the best price, American Delaware for the best security protection, or Panama for the discretion. Clients can have an anonymous company set up for as little as 1000 dollars. For an extra fee CSP provides a sham director for the company, with the purpose of covering up who's really behind it. The primary aim is to conceal the identities of the true company owners. In official statements, CSP can repeatedly state that it does not work directly with end clients, but only with intermediaries, such as banks or asset management companies. In fact, CSR even offers its end clients anonymous email addresses if desired, with fake names such as „Winnie the Pooh" and „Harry Potter", or „Fighter", „Azkaban", „Father", „Daughter", or „Son".
2) Individuals appointed by offshore service provider serve as sham directors for hundreds or even thousands of companies, but have no real decision power. These people sign blank templates for documents or contracts, supposedly without knowing what would be done with their signature and these documents later on. The corresponding contractual details are added to the documents if needed, depending on the CSRs' client's intentions.
3) The general outcome of the scheme is that the company is a black box, i.e. no one sees what is going on inside. To access the money, the offshore company could lend money with a zero interest rate to a company based in the home country of the individual which is also ultimately owned or controlled by the individual or company that is avoiding tax. This individual or company can then extract cash from the recipient company while paying minimal tax.

GATEKEEPRS

Money launderers seek out the advice or services of specialised professionals to help facilitate their financial operations. This trend toward the involvement of various legal and financial experts, or gatekeepers, in money laundering schemes that have been documented previously by the FATF and appears to continue today.

Definition: Gatekeepers are financial and non-financial professionals that provide legal advice, consultancy or legal assistance to Organised Crime Groups and act as intermediaries by giving criminals access to the financial system and facilitating the conduct of their „business". They can either be used or be a part of the criminal organisation. Organised Crime Groups are drawn to these criminal providers due to the perception that these professions are protected from law enforcement scrutiny by professional secrecy privileges, mitigating the risk of being subject to investigations and prosecutions. In simple words, „gatekeepers are individuals that protect the gates of the financial system" (UNODC UN Anti-Corruption Toolkit 2004, FATF Money Laundering 2011).

INTERNATIONAL TRANSFERS VIA OFFICIAL AND UNOFFICIAL FINANCIAL SYSTEMS LIKE HAWALA

The combination of official and unofficial money transfer techniques like MSBs, banking sector, Trade-Based Money Laundering, cash couriers, money collectors, money mules and Informal Value Transfer Systems (IVTS) like Hawala, are used by Organised Crime Groups to move wealth anonymously. Contrary to the small and medium level money laundering areas (migrant smuggling, fraud, motor vehicle crime, payment card fraud and in low level cybercrime and drug trafficking) were Law Enforcement Agencies are capable to investigate and provide a response, in the area of international transfers the only way for Law Enforcement Agencies to obtain the necessary knowledge and information to identify the beneficial owner and to trace international transfers is via a strong cooperation with the private sector, and with banks in particular – major international banks and their networks of correspondent banking.

Financial Intelligence team

Almost all criminal activities yield profits, often in the form of cash, that the criminals then seek to launder through various channels. Money laundering is an offence in its own right, but it is also closely related to other forms of serious and organised crime. In addition to organised criminal groups, professional money launderers perform money laundering services on behalf of others as their core business. The scale of money laundering is difficult to assess, but it is considered to be significant. The Financial Intelligence team (FI) within Europol has a broad mandate in the area of combating money laundering, and provides Member States with intelligence and forensic support to prevent and combat international money laundering activities. The main objective in tracing illegal assets and money laundering is to find the criminals involved, disrupt their associates and confiscate the proceeds of their crimes.

- Is part of Horizontal Operational Support (HOS) and comprises three teams – AP Sustrans, ECAB and the FIU.Net Team;

- provides horizontal and vertical operational support;
- has an important role within continuously developing financial intelligence training efforts within the EU, supplying one-week training on Financial Intelligence to MSs and other key countries on a regular basis;
- it moreover maintains the largest community of users in different platforms and hosts the secretariats for the AMON network and the CARIN network.

Analysis Project Sustrans is Europol's initiative regarding the fight against money laundering. It is an operational platform to support MS on-going cases in the area of money laundering. The only prerequisites to be eligible for support from AP Sustrans are that the case affects two or more Member States and involves a suspected money laundering offence.

In March 2007 Europol was given a full mandate in the matter of money laundering regardless of the predicate offence committed. The purpose of AP Sustrans is to support competent authorities of the Member States in preventing and combating the activities of criminal groups involved in money laundering, in particular through the analysis of information contained in Suspicious Transaction Reports (STRs). This team supports European Union Members States to detect and disrupt criminal cash flows linked to criminality, e.g. those stemming from drug trafficking moving in and out of European Union territory to high-risk destinations and source countries.

AP Sustrans hosts secretariat of AMON the Anti-Money Laundering Operational Network (AMON) is an international network of practitioners working in the area of anti- money laundering investigations.

AMON aims to:

- promote cooperation through providing a network for practitioners in money laundering;
- become an international centre for exchange of knowledge and best practice in the area of money laundering;
- provide capacity building and training in money laundering;
- maintain a secure web-based platform to promote AMON.

The Europol Criminal Assets Bureau encompasses various activities related to asset forfeiture, namely the Camden Asset Recovery Inter-Agency Network (CARIN) secretariat, the Asset Recovery Office (ARO) platform and the analysis project Asset Recovery.

ECAB supports competent authorities of the European Union Member States, and also Third States and organisations in the identification and tracing of criminal proceeds linked to all mandated crime areas of Europol.

The Camden Asset Recovery Inter-Agency Network (CARIN) is an informal network of practitioners in the field of asset recovery. It helps its members to increase their effectiveness in depriving criminals of their ill-gotten assets. CARIN has representatives from 56 countries. With other ARIN type networks in the world, the number of jurisdictions covered is 151.

The ARO platform is a discussion forum for the European Union asset recovery offices. ECAB co-chairs with the EU Commission this platform. Specific topics like the establishment of centralized bank account registers or the freezing of virtual currencies are discussed within the ARO platform.

The AP Asset Recovery supports competent authorities of the Member States and Third States and organisations in the tracing and identification of criminal proceeds linked to the mandated crime areas of Europol.

FIU.net is a decentralised computer network that connects all 28 European Union Financial Intelligence Units (FIUs), who use FIU.net to exchange suspicious transaction reports (STRs). The embedment of FIU.net at Europol aims to improve cooperation between all parties involved in the fight against international money laundering and terrorist financing, in particular strengthening connections with FIUs and the exploitation of the financial intelligence they gather. The FIU.net team functions as the 29th FIU within FIU.net, bringing possibilities for MS Competent Authorities and FIUs to identify connections between the financial intelligence they collect and criminal intelligence stored at Europol.

Main responsibilities of the Financial Intelligence team

Operational and financial analysis reports: for example, reports focusing on intelligence analysis, links analysis, geographical and transaction analysis, social network analysis, dependent on information provided and objectives of the case.

Situation reports: for example, in cases where numerous member states are affected, providing a clear global overview of the groups and phenomenon.

Strategic analysis and knowledge products: non- operational analysis of trends, methods and threats relating to money laundering.

Training: FI provides week-long Financial Intelligence Training courses each year. We also contribute to CEPOL, CEIFAC and ICOFI money laundering courses, both in designing preparatory materials and delivering training.

Financial Intelligence Training – FIT is a week-long course provided each year. The course aims at introducing investigators, analysts, and law enforcement officers to the field of financial intelligence, and to expand their knowledge and capacity in regards of the financial aspects of criminal investigations.

The course objective is:

- to provide knowledge on financial intelligence in the criminal environment;
- engage in challenging exercises on real case scenarios;
- practising with live searches of financial information over the internet;
- to introduce participants to the secrets of financial statements, sophisticated company structures, complex financial instruments, remittance systems and virtual currencies.

Case example: Asset Recovery – successful cooperation between Europol and Poland

On 12-13 June 2016, 100 law enforcement officers from the Polish Asset Recovery Office and tax authorities, supported by a Europol expert, arrested 3 suspects and seized assets, such as cash, luxury motor vehicles and real estate. Overall, 34 searches were carried out in houses, accounting offices and various companies.

A strong collaboration among Polish and German asset recovery offices, supported by Europol's Criminal Assets Bureau played a significant role in identifying key players and gathering information about intra-community supply chain of luxury vehicles.

Between 2015 and 2016, the organised criminal group traded in oil and luxury cars to illegally acquire massive amounts of value added tax (VAT) from the Polish State Treasury. According to the latest figures, the VAT loss for the Polish authorities is estimated at approximately EUR 20 million. The seized criminal assets will be used for the recovery of damages.

The organised crime group used a person to set up a company and to trade in luxury vehicles. He was obliged to paid VAT and excise duty for purchase of 20 luxury cars in total, imported from Germany.

A mobile Europol office was deployed on the field in Wrocław, allowing for real time cross-checks of data on the action day and extraction of evidence from the seized assets.

Jacek Baranowski
Financial Intelligence Group, EUROPOL

Rola i wsparcie Europolu w dochodzeniach finansowych. Współpraca z państwami członkowskimi Unii Europejskiej

Streszczenie

Referat omawia skalę zjawiska prania pieniędzy w krajach Unii Europejskiej. Innowacje technologiczne w systemach komunikacji wraz z coraz bardziej powszechnymi bezgotówkowymi transakcjami finansowymi zapewniają międzynarodowym grupom zajmującym się przestępczością zorganizowaną narzędzia do planowania i popełniania szeregu przestępstw.

Zespół ds. wywiadu finansowego w ramach Europolu zapewnia państwom członkowskim wsparcie wywiadowcze i kryminalistyczne w celu zapobiegania i zwalczania międzynarodowego prania pieniędzy. Do głównych celów zespołu należy identyfikowanie przestępców zaangażowanych w pranie pieniędzy, zakłócenie działań ich wspólników i konfiskata zysków pochodzących z popełnionych przestępstw.

Współpraca między Europolem a krajami Unii Europejskiej, doprowadziła do pomyślnych rezultatów takich jak przejęcie znacznej ilości mienia pochodzącego z przestępstw.

Zorganizowane grupy przestępcze i pranie pieniędzy

Działania w zakresie prania pieniędzy wykrywane i analizowane obecnie przez organy ścigania w Unii Europejskiej charakteryzują się połączeniem zbieżnych elementów, które sprawiają, że zjawisko prania pieniędzy stanowi doskonałą symbiozę tradycji i innowacyjnych rozwiązań. Duża liczba możliwości oferowanych przez nowoczesne systemy komunikacji zapewniła międzynarodowym grupom zajmującym się przestępczością zorganizowaną platformę bez granic, dzięki której interesy przestępcze są planowane, rozwijane i konsolidowane. Temu procesowi towarzyszył rozwój międzynarodowego sektora bankowego, który zmierza obecnie w kierunku szerszego wykorzystania bezgotówkowych instrumentów finansowych, dzięki którym transakcje finansowe mogą być również zawierane na odległość.

Co więcej, nowe możliwości zostały otwarte dzięki zmianom o charakterze społeczno-politycznym, do których doszło w Unii Europejskiej, dzięki której wiele państw zostało zintegrowanych w jeden unikalny organizm polityczny z jednolitym rynkiem i dużymi obszarami państw członkowskich, w których osoby i towary mogą przemieszczać się swobodnie i bez ograniczeń. Brak wewnętrznych granic Unii Europejskiej oraz wprowadzenie waluty euro wraz z nowymi wymogami wynikającymi z wdrożenia trzeciej dyrektywy Unii Europejskiej dotyczącej prania pieniędzy skłoniły zarówno unijne, jak i pozaunijne zorganizowane grupy przestępcze do konsekwentnego zwiększania wykorzystania instrumentów pieniężnych w celu wprowadzania i umiejscawiania dochodów pochodzących z przestępstwa i unikania

wykrycia przez organy ścigania. To właśnie w ramach tego dość złożonego i specyficznego scenariusza przestępstwa polegające na praniu pieniędzy są popełniane przez międzynarodowe grupy przestępcze przebywające na terenie Unii Europejskiej, niezależnie od pochodzenia etnicznego lub geograficznego zaangażowanych grup przestępczych.

Pieniądze pochodzące z przestępstw i pranie pieniędzy

Pranie brudnych pieniędzy umożliwia zorganizowanym grupom przestępczym wprowadzanie dochodów pochodzących z przestępstwa do legalnego obiegu gospodarczego. Niemal wszystkie grupy przestępcze są zmuszone do prania zysków pochodzących z działalności przestępczej; sposób prania brudnych pieniędzy różni się jednak znacznie w zależności od poziomu wiedzy i doświadczenia grupy przestępczej oraz częstotliwości i skali działań związanych z praniem brudnych pieniędzy.

Organizacje kryminalne nieustannie poszukują możliwości wykorzystania najnowszych osiągnięć technologicznych, takich jak kryptowaluty i anonimowe metody płatności. Szybkie przetwarzanie transakcji i mnożenie skutecznych narzędzi anonimizacji są istotnymi przeszkodami w identyfikacji rzeczywistych posiadaczy dochodów z działalności przestępczej. Rosnąca liczba platform i aplikacji on-line oferuje nowe sposoby przekazywania pieniędzy i nie zawsze są one regulowane w takim samym stopniu jak tradycyjni dostawcy usług finansowych.

Osoby zajmujące się praniem pieniędzy w dużym stopniu polegają na oszustwach związanych z dokumentami w celu ułatwienia swojej działalności. Fałszywe dokumenty, takie jak faktury czy sfałszowane dokumenty tożsamości, są wykorzystywane do ukrywania pochodzenia pieniędzy pochodzących z przestępstwa, otwierania kont bankowych lub zakładania spółek fasadowych.

Osoby zajmujące się praniem pieniędzy świadczą usługi zarówno na rzecz organizacji przestępczych, jak i organizacji terrorystycznych.

Najczęstszymi metodami prania pieniędzy są:

Przemyt gotówki: przy pomocy kurierów lub za pośrednictwem poczty i przesyłek pocztowych. **Gotówka** pozostaje głównym obszarem działalności sieci zajmujących się praniem brudnych pieniędzy. Nadal dochodzi do przemytu gotówki przez **kurierów** oraz w coraz większym stopniu za pośrednictwem **poczty i paczek**.

Syndykaty zajmujące się praniem pieniędzy polegają na sieciach pośredników i skomplikowanych technikach prania brudnych pieniędzy. **Syndykaty zajmujące się praniem brudnych pieniędzy** oferują złożone techniki prania pieniędzy i przeprowadzają związane z tym procederem czynności w imieniu zorganizowanych grup przestępczych w zamian za prowizję w wysokości od 5% do 8%.

Pranie brudnych pieniędzy w obrocie handlowym: fałszywe faktury i podrobione dokumenty tożsamości są wykorzystywane przez spółki fasadowe należące do grup przestępczości zorganizowanej w celu ukrycia funduszy przestępczych. **Pranie brudnych pieniędzy w obrocie handlowym** jest bardzo skutecznym sposobem ukrywania funduszy pochodzących z przestępstwa poprzez manipulowanie lub fałszowanie zakupów lub sprzedaży przy użyciu podwójnego fakturowania, fałszywego fakturowania przez firmy należące do grupy przestępczości zorganizowanej, jej współpracowników i krewnych.

Nowe metody płatności, takie jak kryptowaluty i anonimowe metody płatności, są istotnymi przeszkodami w identyfikacji rzeczywistych posiadaczy dochodów pochodzących z przestępstwa.

Nowe metody płatności, takie jak wymiana kryptowaluty, karty przedpłacone, płatności online i bony internetowe stale się rozwijają i są generalnie uregulowane w dużo mniejszym stopniu niż tradycyjne metody płatności.

Podmioty prawne występujące w systemach prania pieniędzy:

USŁUGODAWCY FIRMOWI

Zgodnie ze sprawozdaniem FATF z 2010 roku w sprawie prania pieniędzy przy wykorzystaniu funduszy powierniczych i firmowych dostawców usług, spółki tego rodzaju odgrywają kluczową rolę w globalnej gospodarce jako pośrednicy finansowi, zapewniając ważne powiązania między instytucjami finansowymi a wieloma ich klientami. Zapewniają one często nieocenioną pomoc klientom w zarządzaniu ich finansami, a tym samym mogą mieć istotny wpływ na przepływy transakcyjne za pośrednictwem systemu finansowego.

Dostawcy usług korporacyjnych (CSP) są zazwyczaj reprezentowani przez prawników i ekspertów finansowych. Eksperci finansowi mogą być:

1) podmiotami działającymi jako przedstawiciele osób prawnych, których usługi obejmują zostanie lub zatrudnienie osób trzecich w charakterze akcjonariuszy powierniczych na rzecz innej osoby;
2) podmiotami działającymi w charakterze dyrektora (lub zatrudniające osobę trzecią w celu pełnienia obowiązków dyrektora) bądź sekretarza spółki kapitałowej, wspólnika spółki osobowej lub osoby trzeciej zajmującej podobne stanowisko w stosunku do innych osób prawnych;
3) podmiotami udostępniającymi siedzibę statutową, adres siedziby, miejsce prowadzenia działalności lub zakwaterowania, adres administracyjny lub korespondencyjny adres spółki osobowej lub innej osoby prawnej lub układu;
4) podmiotami działającymi w charakterze w charakterze osoby upoważnionej (lub zlecające osobie trzeciej działanie w charakterze takiej osoby).

Istnieje istotny związek pomiędzy CSP a podmiotami w zagranicznych rajach podatkowych, ponieważ większość firm specjalizujących się we wspomnianych powyżej usługach jest zarejestrowana w tego typu miejscach. Wynika z tego, że:

1) Wszystkie kwestie administracyjne są obsługiwane przez spółkę zarejestrowaną w raju podatkowym, na przykład dobrze znaną ze skandalu Panama Papers spółkę Mossack Fonseca. Pomagają one nie tylko w załatwianiu formalności, ale również umożliwiają wybór najbardziej odpowiedniego raju podatkowego w zależności od celu i oczekiwań klienta: Brytyjskie Wyspy Dziewicze oferują najlepszą cenę, amerykański stan Delaware zapewnia najlepszą ochronę bezpieczeństwa, może to także być Panama – jeśli klientowi zależy na dyskrecji. Klienci mogą stać się właścicielami anonimowej spółki za zaledwie 1000 dolarów. Za dodatkową opłatą CSP zapewniają także usługi osoby odgrywającej rolę dyrektora spółki, której celem jest ukrycie tego, kto naprawdę stoi za daną działalnością. Głównym celem jest ukrycie tożsamości prawdziwych właścicieli spółek. W oficjalnych oświadczeniach CSP często znaleźć

można informacje na temat tego, że tego rodzaju spółki nie współpracują bezpośrednio z klientami końcowymi, lecz jedynie z pośrednikami, takimi jak banki lub spółki zarządzające aktywami. W rzeczywistości CSR oferują nawet swoim klientom końcowym anonimowe adresy e-mailowe dostępne na żądanie, z nazwami kont takimi jak „Kubuś Puchatek", „Harry Potter", „Azkaban", „Ojciec", „Córka" lub „Syn".

2) Osoby fizyczne wyznaczone przez dostawcę usług znajdującego się w raju podatkowym pełnią funkcję dyrektorów – pozorantów dla setek, a nawet tysięcy firm, jednak nie mają oni rzeczywistej władzy decyzyjnej. Osoby te podpisują puste szablony dokumentów lub kontraktów, nie wiedząc co stanie się z ich podpisem i podpisanymi dokumentami w późniejszym czasie. W razie potrzeby do dokumentów dołączane są odpowiednie szczegóły umowy, w zależności od intencji klientów CSR.
3) Ogólnym rezultatem tego procederu jest fakt, że przedsiębiorstwo staje się niejako czarną skrzynką, tj. nikt nie widzi tego, co dzieje się wewnątrz. Aby uzyskać dostęp do tych pieniędzy, przedsiębiorstwo zagraniczne może pożyczać środki bez odsetek spółce zarejestrowanej w kraju pochodzenia osoby fizycznej, które stanowi również własność lub jest kontrolowane przez osobę fizyczną lub przedsiębiorstwo unikające opodatkowania. Ta osoba fizyczna lub przedsiębiorstwo może wówczas pobierać gotówkę od przedsiębiorstwa otrzymującego pomoc, płacąc jednocześnie minimalny podatek.

STRAŻNICY (GATEKEEPERS)

Przestępcy zajmujący się praniem pieniędzy zwracają się w celu uzyskania porad lub specjalistycznych usług świadczonych przez specjalistów, które mogą ułatwić im operacje finansowe. Ta tendencja do angażowania różnych ekspertów prawnych i finansowych – strażników – w programy prania brudnych pieniędzy została już wcześniej udokumentowana przez FATF i wydaje się być w dalszym ciągu aktualna.

Definicja: strażnicy (gatekeepers) to specjaliści finansowi i niefinansowi, którzy doradzają grupom przestępczości zorganizowanej i działają jako pośrednicy, dając przestępcom dostęp do systemu finansowego i ułatwiając prowadzenie „działalności". Przestępcy mogą wyłącznie korzystać z ich usług lub też osoby te mogą stanowić część organizacji przestępczej. Zorganizowane grupy przestępcze są zainteresowane ich usługami ze względu na przekonanie, że zawody te są chronione przed kontrolą organów ścigania dzięki przywilejom związanym z tajemnicą zawodową, co zmniejsza ryzyko dochodzenia i ścigania. Mówiąc prosto, „strażnicy to osoby, które chronią bramy systemu finansowego" (UNODC UN Anti-Corruption Toolkit 2004, FATF Money Laundering 2011).

PRZEKAZY MIĘDZYNARODOWE ZA POŚREDNICTWEM OFICJALNYCH I NIEOFICJALNYCH SYSTEMÓW FINANSOWYCH, TAKICH JAK HAWALA

Połączenia oficjalnych i nieoficjalnych technik przekazywania pieniędzy, takich jak przedsiębiorstwa świadczące usługi w zakresie zarządzania pieniędzmi, sektor bankowy, pranie brudnych pieniędzy w obrocie handlowym, kurierzy gotówki, odbiorcy pieniędzy, muły i nieformalne systemy transferu wartości (IVTS), takie jak *Hawala*, są wykorzystywane przez grupy przestępcze w celu anonimowego przenoszenia majątku. W przeciwieństwie do prania

brudnych pieniędzy o małym i średnim zakresie (przemyt przez migrantów, nadużycia finansowe, przestępczość związana z pojazdami silnikowymi, oszustwa związane z kartami płatniczymi oraz cyberprzestępczość niskiego szczebla i handel narkotykami), w przypadku których organy ścigania są w stanie samodzielnie prowadzić dochodzenia i odpowiadać na te wyzwania, w dziedzinie międzynarodowych transferów pieniędzy jedynym sposobem uzyskania przez organy ścigania wiedzy i informacji niezbędnych do zidentyfikowania rzeczywistego posiadacza oraz śledzenia przelewów międzynarodowych jest ścisła współpraca z sektorem prywatnym i bankami – w szczególności z głównymi bankami międzynarodowymi i ich sieciami korespondentów.

Zespół ds. wywiadu finansowego

Niemal wszystkie działania przestępcze przynoszą zyski, często w formie gotówki, które przestępcy starają się następnie prać przy pomocy wielu kanałów. Pranie pieniędzy jest samo w sobie przestępstwem, ale jest również ściśle związane z innymi formami poważnej i zorganizowanej przestępczości. Oprócz zorganizowanych grup przestępczych, osoby zajmujące się zawodowo praniem brudnych pieniędzy świadczą te usługi na rzecz innych podmiotów w ramach swojej podstawowej działalności. Trudno jest oszacować skalę procederu prania brudnych pieniędzy, ale uznaje się ją za znaczącą. Zespół wywiadu finansowego (FI) działający w ramach Europolu posiada szeroki zakres uprawnień w dziedzinie zwalczania prania pieniędzy i zapewnia państwom członkowskim wsparcie wywiadowcze i kryminalistyczne w celu zapobiegania i zwalczania międzynarodowego prania pieniędzy. Głównym celem wykrywania nielegalnego majątku i prania brudnych pieniędzy jest odnalezienie przestępców, zakłócenie działań ich wspólników i konfiskata zysków pochodzących z popełnionych przestępstw.

- Jest częścią Horyzontalnego Wsparcia Operacyjnego (HOS) i składa się z trzech zespołów: AP Sustrans, ECAB i FIU.Net Team;
- zapewnia poziome i pionowe wsparcie operacyjne;
- odgrywa ważną rolę w ustawicznym rozwoju działań szkoleniowych w zakresie wywiadu finansowego w UE, regularnie organizując tygodniowe szkolenia na temat wywiadu finansowego dla państw członkowskich i innych kluczowych krajów;
- ponadto utrzymuje największą społeczność użytkowników na różnych platformach i udostępnia sekretariaty sieci AMON i sieci CARIN.

Projekt analityczny AP Sustrains jest inicjatywą Europolu dotyczącą walki z praniem brudnych pieniędzy. Jest to platforma operacyjna wspierająca państwa członkowskie w bieżących i trwających sprawach dotyczących prania pieniędzy. Jedynymi warunkami wstępnymi, które kwalifikują dane państwo do uzyskania wsparcia ze strony AP Sustrans jest to, że sprawa musi dotyczyć dwóch lub więcej państw członkowskich i wiąże się z podejrzeniem popełnienia przestępstwa prania pieniędzy.

W marcu 2007 roku Europol otrzymał pełne uprawnienia związane ze zwalczaniem prania pieniędzy niezależnie od popełnionego przestępstwa źródłowego.

Celem programu AP Sustrans jest wspieranie poszczególnych organów państw członkowskich w zapobieganiu i zwalczaniu działalności grup przestępczych zajmujących się praniem brudnych pieniędzy, w szczególności poprzez analizę informacji zawartych w sprawozdaniach

z podejrzanych transakcji (STR). Zespół ten wspiera państwa członkowskie Unii Europejskiej w wykrywaniu i zakłócaniu kryminalnych przepływów pieniężnych związanych z przestępczością, np. przepływów wynikających z handlu narkotykami pieniędzy przemieszczanych z i na terytorium Unii Europejskiej, do miejsc docelowych wysokiego ryzyka i krajów pochodzenia.

AP Sustrans jest gospodarzem sekretariatu AMON – Sieci Operacyjnej Przeciw Praniu Pieniędzy (AMON), która jest międzynarodową siecią praktyków pracujących w dziedzinie dochodzeń w sprawach przeciwdziałania praniu brudnych pieniędzy.

AMON stawia sobie za cel:

- promowanie współpracy poprzez budowanie sieci kontaktów dla praktyków zajmujących się praniem pieniędzy;
- stanie się międzynarodowym centrum wymiany wiedzy i najlepszych praktyk w dziedzinie prania brudnych pieniędzy;
- zapewnienie budowania potencjału i szkoleń w zakresie prania pieniędzy;
- utrzymanie bezpiecznej platformy internetowej promującej AMON.

Biuro ds. odzyskiwania mienia Europolu (Criminal Assets Bureau) podejmuje różne działania i projekty związane z zajmowaniem mienia, przede wszystkim są to sekretariat Międzyagencyjnej Sieci Odzyskiwania Mienia Camden (CARIN), platformę biura ds. odzyskiwania mienia (ARO) oraz projekt analityczny dotyczący odzyskiwania mienia.

ECAB wspiera właściwe organy państw członkowskich Unii Europejskiej, a także państwa trzecie i organizacje zewnętrzne w identyfikowaniu i wykrywaniu korzyści pochodzących z przestępstwa związanych ze wszystkimi obszarami działalności przestępczej, którymi zajmuje się Europol na mocy przydzielonych uprawnień.

Międzyagencyjna Sieć Odzyskiwania Mienia Camden (CARIN) jest nieformalną siecią praktyków pracujących w dziedzinie odzyskiwania mienia. Sieć pomaga jej członkom zwiększyć ich skuteczność w pozbawianiu przestępców ich pozyskanego w nielegalny sposób majątku. CARIN ma przedstawicieli pochodzących z 56 krajów. Wraz z innymi sieciami typu ARIN, ogólna liczba objętych nimi jurysdykcji na całym świecie wynosi 151.

Platforma ARO jest forum dyskusyjnym dla biur ds. odzyskiwania mienia w Unii Europejskiej. ECAB przewodniczy platformie wspólnie z Komisją Europejską. W ramach platformy ARO omawiane są konkretne tematy, takie jak utworzenie scentralizowanych rejestrów kont bankowych czy zamrożenie wirtualnych walut.

AP Asset Recovery wspiera właściwe organy państw członkowskich i państw trzecich oraz organizacje w zakresie wykrywania i identyfikacji dochodów pochodzących z przestępstw związanych z obszarami działalności przestępczej, którymi zajmuje się Europol na mocy przydzielonych uprawnień.

FIU.net jest zdecentralizowaną siecią komputerową, która łączy wszystkie 28 Jednostek Wywiadu Finansowego Unii Europejskiej (FIU), które wykorzystują FIU. net do wymiany informacji o podejrzanych transakcjach (STR). Włączenie FIU.net w struktury Europolu ma na celu poprawę współpracy między wszystkimi stronami zaangażowanymi w walkę z międzynarodowym praniem pieniędzy i finansowaniem terroryzmu, w szczególności wzmocnienie powiązań z jednostkami wywiadu finansowego i wykorzystanie gromadzonych

przez nie informacji finansowych. Zespół FIU.net działa jako 29. jednostka wywiadu finansowego w ramach FIU.net, dając właściwym organom państw członkowskich i jednostkom wywiadu finansowego możliwość zidentyfikowania powiązań między gromadzonymi przez nie informacjami finansowymi i danymi wywiadowczymi gromadzonymi w Europolu.

Główne obowiązki zespołu ds. wywiadu finansowego

Sprawozdania z analizy operacyjnej i finansowej: na przykład sprawozdania koncentrujące się na analizach wywiadowczych, analizach linków, analizach geograficznych i analizach transakcji, analizach sieci społecznościowych, w zależności od dostarczonych informacji i celów sprawy.

Raporty sytuacyjne: na przykład w przypadkach, gdy dany problem dotyczy wielu państw członkowskich; raport powinien zapewniać jasny i ogólny przegląd grup i zjawiska

Analiza strategiczna i produkty wiedzy: nieoperacyjna analiza tendencji i trendów, metod i zagrożeń związanych z praniem brudnych pieniędzy.

Szkolenie FI organizuje co roku tygodniowe szkolenia z zakresu wywiadu finansowego. Uczestniczymy również w kursach szkoleniowych CEPOL, CEIFAC i ICOFI poświęconych praniu brudnych pieniędzy, zarówno przygotowując materiały, jak również prowadząc szkolenia.

Szkolenie w zakresie wywiadu finansowego – FIT to tygodniowy kurs organizowany co roku. Kurs ma na celu wprowadzenie śledczych, analityków i funkcjonariuszy organów ścigania w obszar wywiadu finansowego oraz poszerzenie ich wiedzy i umiejętności w zakresie finansowych aspektów dochodzeń karnych.

Kurs ma na celu:

- dostarczanie wiedzy na temat wywiadu finansowego w środowisku kryminalnym.
- zaangażowanie funkcjonariuszy w trudne ćwiczenia dotyczące rzeczywistych scenariuszy przypadku.
- ćwiczenie w wyszukiwaniu na żywo informacji finansowych za pośrednictwem internetu,
- zapoznanie uczestników z tajemnicą sprawozdań finansowych, wyrafinowanymi strukturami firm, złożonymi instrumentami finansowymi, systemami przekazów pieniężnych i walutami wirtualnymi.

Studium przypadku: Odzyskiwanie mienia – udana współpraca pomiędzy Europolem i Polską

W dniach 12-13 czerwca 2016 roku 100 funkcjonariuszy organów ścigania z polskiego Biura Odzyskiwania Mienia i organów podatkowych, wspieranych przez eksperta Europolu, aresztowało 3 podejrzanych i zatrzymało mienie, takie jak gotówka, luksusowe samochody i nieruchomości. W sumie przeprowadzono 34 rewizje w domach, biurach rachunkowych i spółkach.

Ścisła współpraca pomiędzy polskimi i niemieckimi biurami ds. odzyskiwania mienia, wspierana przez Biuro ds. odzyskiwania mienia Europolu, odegrała znaczącą rolę w identyfikacji kluczowych podmiotów i gromadzeniu informacji o wewnątrzwspólnotowym łańcuchu dostaw luksusowych pojazdów.

W latach 2015-2016 zorganizowana grupa przestępcza prowadziła handel ropą naftową i luksusowymi samochodami w celu nielegalnego uzyskania od Skarbu Państwa RP ogromnych

kwot zwrotów podatku VAT. Zgodnie z najnowszymi danymi liczbowymi strata podatku VAT związana z tym przestępstwem szacowana jest na około 20 mln €. Zajęte mienie pochodzące z działalności przestępczej zostanie wykorzystane w celu wypłaty odszkodowania.

Zorganizowana grupa przestępcza wykorzystywała osobę do założenia firmy i handlu luksusowymi pojazdami. Osoba ta była zobowiązana do zapłaty podatku VAT i akcyzy za zakup 20 luksusowych samochodów importowanych z Niemiec.

Na terenie Wrocławia uruchomiono mobilne biuro Europolu, które umożliwiło w czasie rzeczywistym kontrolę krzyżową danych w dniu akcji oraz pozyskiwanie dowodów z zajętego majątku.

podkom. SC Kamilla Siwek
Dział ds. Wyrobów Energetycznych, Śląski Urząd Celno-Skarbowy w Katowicach

Zagrożenia w obrocie krajowym i międzynarodowym wyrobami energetycznymi

Streszczenie

W trakcie międzynarodowej konferencji pt. „Ochrona interesów finansowych Unii Europejskiej – wspólne zobowiązania i wyzwania" w zaplanowanym przez organizatorów temacie „Zagrożenia w obrocie wyrobami energetycznymi (obrót krajowy i międzynarodowy)" przedstawiciel Śląskiego Urzędu Celno-Skarbowego – funkcjonariusz Służby Celno-Skarbowej przedstawił prezentację pt. „Nieprawidłowości identyfikowane przez Służbę Celną/Krajowa Administrację Skarbową w obszarze paliw". W trakcie prelekcji omówione zostały:

- udział paliw ciekłych w dochodach budżetowych Skarbu Państwa (akcyza, VAT),
- skala konsumpcji paliw ciekłych w Polsce,
- źródła pochodzenia paliw ciekłych,
- podstawowe zagrożenia identyfikowane przez KAS w obrocie paliwami,
- regulacje prawne wprowadzone w celu zniwelowania szarej strefy w obrocie paliwami,
- elektroniczny system monitorowania drogowego przewozu towarów SENT.

Na początku chciałabym zwrócić uwagę na jedną kwestię. Mianowicie od 1 marca 2017 r. jesteśmy instytucją zreformowaną. Powstaliśmy na gruncie trzech instytucji: administracji podatkowej, kontroli skarbowej oraz Służby Celnej. Jestem celniczką i pewne aspekty związane z przeszłością, z rozpoznawaniem przestępczości paliwowej przez Służbę Celną będę omawiała w oparciu o działania byłej Służby Celnej, która została wchłonięta przez Krajową Administrację Skarbową (KAS) kontynuującą zadania w tym zakresie. Jednak będzie mi po prostu łatwiej używać dawnego nazewnictwa.

Źródła pochodzenia paliw ciekłych i skala konsumpcji w Polsce

Na początku ogólnie przybliżę i umiejscowię paliwa w aspekcie gospodarczym. Źródłem paliw, głównie oleju napędowego, ale też pozostałych paliw silnikowych w Polsce, jest niemal w ¾ produkcja krajowa, w krajowych rafineriach. Niemal ¼ obrotu stanowi napływ paliw do Polski z importu z Rosji i Białorusi, ale również z nabycia wewnątrzwspólnotowego z Niemiec i Litwy. W oparciu o dane, które publikowane są w corocznych raportach przez Polską Organizację Paliw i Handlu Naftowego (POPiHN), finalna konsumpcja paliw w Polsce przedstawia się następująco:

- 17 mld litrów oleju napędowego,
- 5 mld litrów benzyny,
- 4 mld LPG,
- 1 mld olej opałowy.

POPiHN w swoich raportach dotyczących ogólnej konsumpcji paliw umieszcza dane w oparciu o krajową produkcję, jak również o import i nabycia wewnątrzwspólnotowe. Za POPiHN można stwierdzić, że ¼ ilości skonsumowanego w Polsce oleju napędowego pochodzi z importu i nabyć wewnątrzwspólnotowych. W przypadku benzyny ta proporcja jest zdecydowanie inna, gdyż większość benzyny na rynku jest produkcji krajowej. W przypadku płynnego gazu większość pochodzi z importu, natomiast barwiony olej opałowy jest produkowany w Polsce i barwiony w polskich składach podatkowych. Nie jest przywożony do Polski z zagranicy.

Udział paliw ciekłych w dochodach budżetowych Skarbu Państwa

Paliwa zajmują znaczące miejsce w dochodach budżetu państwa. Kwoty jakie zostały zaplanowane w ustawie budżetowej na rok 2017 z tytułu wpływów podatkowych od paliw to przeszło 3 mld zł. Większość podatku akcyzowego jest pobierana od paliw, następnie od wyrobów tytoniowych i alkoholowych. Jeżeli chodzi o ogólny dochód budżetu państwa w tym zakresie to należy stwierdzić, że podatek akcyzowy od paliw wynosi 9%, natomiast podatek VAT pobierany z tytułu handlu paliwami to 10% wartości. Inne podatki to blisko 80% wpływów. Jak łatwo można wyliczyć, blisko 1/5 dochodów podatkowych państwa stanowią wpływy podatków od paliw (akcyza i podatek VAT). W przypadku wyrobów energetycznych akcyza od paliw stanowi większość. Na dalszym miejscu znajduje się gaz i wyroby gazowe, natomiast akcyza od pozostałych wyrobów energetycznych (oleje smarowe, olej opałowy i wyroby węglowe) stanowi niewielki procent. Przeszło 90% podatku akcyzowego w Polsce pobierane jest od paliw, czyli oleju napędowego i benzyn.

Jeśli chodzi o strukturę cen, to przeszło 50% wartości ceny paliw na stacjach paliw w Polsce stanowią podatki. Wartość wyrobów, to w zależności od wyrobu, od 40 do 50% (w przypadku gazu) ceny detalicznej. Największy zysk z tytułu wprowadzania do obrotu gazu generują dla siebie dystrybutorzy LPG. Pozostałe zyski plasują się na poziomie 3% ceny paliwa.

Podstawowe zagrożenia identyfikowane przez KAS w obrocie paliwami

Wysokie podatki, stosunkowo niewielka marża w cenie detalicznej, wyrób popularny na rynku to najważniejsze czynniki wpływające na próby unikania podatków i generowania większych zysków poprzez nielegalne działania.

Na polskim rynku w obrocie handlowym paliwami krajowym i wspólnotowym rozróżnia się 4 podstawowe obszary ryzyka generujące uszczuplenia podatkowe:

1. nabycie wewnątrzwspólnotowe paliw silnikowych za pośrednictwem **zarejestrowanych odbiorców -** do niedawna bardzo duże ryzyko, generujące bardzo duże uszczuplenia w podatku VAT,
2. szeroko rozumiany obrót handlowy **olejami smarowymi**,

3. zmiana przeznaczenia i zużycie do napędu oleju opałowego, poddanego wcześniej procesowi nielegalnego odbarwienia,
4. wprowadzanie do obrotu paliwa z przemytu z krajów trzecich.

Ryzyko, które obecnie zostało zmianami w przepisach zminimalizowane, to proceder polegający na nabyciu wewnątrzwspólnotowym paliwa za pośrednictwem tzw. **zarejestrowanego odbiorcy**. Za pośrednictwem zarejestrowanych odbiorców, podmioty które sprowadzały z zagranicy paliwo na swoją rzecz, wprowadzały go na terytorium kraju z zapłaconym podatkiem akcyzowym, ale z pominięciem podatku VAT. Problem wyłudzeń VAT jest problemem nie tylko polskim. Jest to problem całej UE. Z danych hiszpańskiej służby podatkowej wynika, że w latach 2015/2016 w oparciu o śledztwa prowadzone przez hiszpańską służbę podatkową, w porozumieniu z innymi służbami i instytucjami, ujawniono przypadki uszczupleń podatkowych w wysokości 157 mln euro. Siedem innych krajów UE wskazało w rocznym raporcie fiskalnym problemy wynikające z uszczupleń z tytułu obrotu olejami mineralnymi. Krajów tych może być jednak znacznie więcej, ponieważ obrót olejami mineralnymi zawsze obarczony jest dużym ryzykiem uszczupleń podatkowych.

W przypadku oleju opałowego cały czas istnieje ryzyko jego odbarwiania i nielegalnego wprowadzania do obrotu na stacjach paliw. Przywóz paliw z krajów trzecich, zza naszej wschodniej granicy, jest na bieżąco kontrolowany. Przemyt paliwa w bakach, przerobionych zbiornikach i kanistrach nie generuje dużych uszczupleń podatkowych, niemniej zagraża legalnym dystrybutorom paliw i zakłóca uczciwą konkurencję.

Ryzyko związane z **olejami smarowymi**, trzeba rozpatrywać natomiast w dwojaki sposób. Mianowicie oleje smarowe są to wyroby, które potocznie kojarzą się z olejami silnikowymi, hydraulicznymi, przekładniowymi. Są to wyroby, które jedynie w Polsce zostały objęte podatkiem akcyzowym. Obecnie nieco zmienia się prawodawstwo krajów UE i niektóre kraje opodatkowały bądź wprowadziły kontrolę przemieszczania tych wyrobów. Ponieważ przywóz olejów smarowych do Polski odbywa się poza unijnym systemem przemieszczania wyrobów akcyzowych w zawieszonej akcyzie (EMCS) i należy zgłosić zamiar nabycia wewnątrzwspólnotowego właściwemu organowi podatkowemu – przywóz do kraju oleju smarowego bez zapłaconej akcyzy wydaje się stosunkowo prosty.

W katalogu olejów smarowych wyróżnia się również oleje smarowe tzw. niskolepkościowe i preparaty smarowe niskolepkościowe, produkowane z oleju napędowego, co umożliwia zmianę przeznaczenia i zużycie do celów napędowych.

W roku 2008 zidentyfikowany został nagły wzrost produkcji tego rodzaju olejów pod różnymi nazwami handlowymi, jednak o takim samym składzie taryfikacyjnym. Ponieważ wspólnotowa taryfa celna dopuszcza klasyfikowanie do olejów smarowych wyroby zawierające nawet 90% oleju napędowego, to składy podatkowe opuszczały wyroby, które mogły być niemal wprost lub po zwykłym skomponowaniu używane do silników spalinowych. Profil producentów takich wyrobów był również stosunkowo prosty. Były to mianowicie podmioty, które sprowadzały olej napędowy w zawieszonej akcyzie. Do oleju napędowego dodawany był olej bazowy i w niewielkiej ilości dodatek smarny i powstawał produkt, który zgodnie z literą prawa mógł być zakwalifikowany jako olej smarowy. Pod taką postacią wyrób był sprzedawany bez podatku akcyzowego zagranicznym odbiorcom. Składy podatkowe,

które zaczęły się parać tym procederem przeznaczały całość produkcji na rynek krajów Unii Europejskiej. Początkowo przedmiotowe oleje smarowe, pochodzące z fikcyjnej dostawy wewnątrzwspólnotowej trafiały na krajowe stacje paliw jako olej napędowy. Proceder w efekcie podejmowanych przez SC, UKS i Policję czynności ewoluował i nieuczciwe podmioty wykorzystywały transakcje trójstronne i odsprzedaż do kolejnych krajów UE, co uniemożliwiało weryfikację u ostatecznego nabywcy i ustalenie sposobu zużycia. W konsekwencji działań podejmowanych przez polskie i zagraniczne służby celne, skarbowe oraz dochodzeniowo-śledcze ujawniano przypadki wprowadzania olejów smarowych do obrotu jako olej napędowy na terenie kraju oraz innych krajów członkowskich UE. Ponieważ Polska dysponowała najlepszym materiałem analitycznym w zakresie olejów smarowych, z inicjatywy polskiej Służy Celnej, a później również węgierskiej służby celnej, w roku 2011 na forum krajów V4 zawiązała się grupa robocza, która została powołana w celu przygotowania materiału analitycznego do KE, tak aby oleje smarowe objąć kontrolą przemieszczania i wciągnąć w system EMCS. Rozwiązanie takie umożliwiałoby kontrolę przemieszczanych olejów smarowych w obrocie wewnątrzwspólnotowym.

Pomimo prac ww. grupy w ramach państw V4 Europejska Komisja Akcyzowa nie zgodziła się na objęcie tych wyrobów kontrolą przemieszczania. Problem pozostaje więc nadal nierozwiązany na rynku ogólnoeuropejskim. W Polsce sytuacja wygląda pod tym względem nieco korzystniej dzięki przyjętym rozwiązaniom legislacyjnym.

Regulacje prawne wprowadzone w celu ograniczenia szarej strefy w obrocie paliwami

Od roku 2012 organizacja POPiHN podnosiła sukcesywnie prognozy dot. szarej strefy paliw w naszym kraju. Początkowo było to ok. 6-7 procent, podczas kiedy w roku 2015 bito już na alarm, ponieważ procent ten wzrósł do prawie 10. Należało więc podjąć działania zmierzające do ograniczenia szarej strefy. Pojawiły się więc nowe regulacje oraz zostały zintensyfikowane kontrole podmiotów paliwowych, jak również zwiększano systematycznie liczbę kontroli prowadzonych na drogach, czyli ilość kontroli transportu w czasie rzeczywistym. W roku 2016 zostały wprowadzone zmiany nazwane „pakietem paliwowym", na podstawie których wprowadzony został m.in. obowiązek zapłaty podatku VAT w momencie nabycia wewnątrzwspólnotowego. Na podstawie danych POIHN wynika, że wprowadzenie zmian legislacyjnych doprowadziło do wzrostu legalnej konsumpcji w Polsce, co oznacza znaczące ograniczenie szarej strefy w Polsce. Na podstawie porównania danych z pierwszej połowy roku 2016 i 2017 zauważono wyraźny wzrost konsumpcji oleju napędowego. Następną regulacją, jaką wprowadzono był tzw. pakiet energetyczny - zmiana w prawie energetycznym, która uporządkowała krajowy rynek, ograniczając możliwość prowadzenia działalności w zakresie paliw tylko dla podmiotów krajowych (posiadających na terytorium RP siedzibę lub oddział). Kolejną regulacją, która została wprowadzona w marcu br. jest monitorowanie transportów drogowych. Ustawą z dnia 9 marca 2017 r. o systemie monitorowania drogowego przewozu towarów wprowadzono obowiązek monitorowania/rejestrowania w elektronicznym systemie przewozu towarów objętych min. pozycjami CN 2207 nieoznaczonych znakami akcyzy, 2707, 2710, 2905, 2917, 3403, 3811, 3814 zawierających alkohol etylowy, 3824 oraz 3826, jeżeli masa brutto przesyłki towarów objętych tymi pozycjami przekracza 500 kg lub jej objętość

przekracza 500 litrów. Rozporządzeniem Ministra Rozwoju i Finansów z dnia 13 czerwca 2017 r. w sprawie towarów, których przewóz jest objęty systemem monitorowania drogowego przewozu towarów (które weszło w życie 22 września 2017 r.) wprowadzono obowiązek rejestrowania przewozu towarów objętych pozycjami CN od 1507 do 1516 i 1517, z wyłączeniem margaryny oraz margaryny płynnej jeżeli masa brutto przesyłki przekracza 500 kg lub jej objętość przekracza 500 litrów.

1st lt. Kamilla Siwek

The Customs and Revenue Service, Energy Products Department, Silesian Customs and Revenue Office in Katowice

Threats in trading of energy products (domestic and international trade)

Abstract

During the international conference "Protection of the financial interests of the EU – common obligations and challenges", in the section planned by the organisers for the subject of "Threats in trading of energy products (domestic and international trade)", a Customs and Revenue Service officer representing the Silesian Customs and Revenue Office will present a paper titled "Irregularities identified by the Customs Service/National Revenue Administration in the area of fuels". The presentation will discuss:

- share of liquid fuels in revenues of the State Treasury's budget (excise duty, VAT),
- scale of liquid fuels consumption in Poland,
- sources of liquid fuels,
- main risks identified by the National Revenue Administration (KAS) in the trade of liquid fuels,
- legal regulations introduced to eliminate grey economy in the trade of liquid fuels,
- electronic system of monitoring of the road carriage of goods (SENT).

I would like to show you my presentation regarding violations of law in the trade of fuels. To start with, I wish to draw your attention to one thing. We have been operating as a reformed institution since 1 March 2017. Our service was established by amalgamation of three authorities: tax administration, tax control and Customs Service. As a customs officer, I am going to discuss certain aspects from the past, namely identification of fuel crime by the Customs Service, on the basis of operations conducted by the Customs Service, which was incorporated into the National Revenue Administration (Polish: Krajowa Administracja Skarbowa, KAS) which continues the tasks in this area. I will simply find it easier to use the old terminology.

Sources and scale of consumption of liquid fuels in Poland

To start my presentation, I wish to give you a general picture of fuels in the context of economy. Fuels, mainly diesel fuel, but also other engine fuels in Poland, account for nearly ¾ of the domestic production by the country's refineries. Nearly ¼ of the trade is generated by imports from Russia and Belarus, but also intra-Community acquisitions from Germany and Lithuania. According to data published in annual reports by the Polish Organisation of Oil Industry and Trade (Polish: Polska Organizacja Przemysłu i Handlu Naftowego, POPiHN), overall fuel consumption in Poland presents as follows:

- 17 billion litres of diesel fuel,
- 5 billion litres of gasoline,
- 4 billion of LPG,
- 1 billion of heating oil.

In its reports on overall fuel consumption, the POPiHN presents data based on domestic production as well as imports and intra-Community acquisitions. Based on data provided by the POPiHN, it can be said that ¼ of diesel fuel consumed in Poland comes from import and intra-Community acquisitions. The share of gasoline is clearly different, as majority of gasoline on the market is produced in the country. As for liquefied petroleum gas, most of it comes from import, while coloured heating oil is produced in Poland and coloured in Polish tax warehouses. It is not imported to Poland.

Share of liquid fuels in revenues of the State Treasury's budget

Fuels have a significant share in the State budget's revenues. Tax revenues from fuels planned in the 2017 Budget Act exceed PLN 3 billion. The largest share of excise duty is charged on fuels, followed by tobacco products and alcoholic beverages. As for the overall revenue of the State budget from taxes, it should be said that the excise duty rate on fuels is 9%, while VAT charged on fuels accounts for 10%. Other taxes account for nearly 80% of the revenues. It can be easily calculated that nearly 1/5 of the State's tax revenues are tax revenues from fuels (excise duty and VAT). The excise duty on fuels has the largest share in the energy product's total, followed by gas and gas products, while the excise duty on other energy products (lubricating oils, heating oil and coal products) is only a small percentage. More than 90% of the excise duty in Poland is charged on fuels, i.e. diesel fuel and gasoline.

As for the price structure, more than 50% of the fuel price at petrol stations in Poland is taxes. The value of the product is, depending on the type, between 40 and 50% (for gas) of the retail price. The largest profit from trading of gas is generated by LPG distributors. In other cases, the profit is at 3% of the fuel price.

Main risks identified by the KAS in the trade of liquid fuels

High taxes, relatively small margin in the retail price, a product that is popular on the market – these are the main factors that encourage attempts to evade taxes and generate bigger profits through illegal activities.

On the Polish market, in the domestic and Community trade of fuels, there are 4 main risks areas that generate tax shortfalls:

1. intra-Community acquisition of engine fuels through **registered consignees –** up until recently, a very high risk generating very large VAT shortfalls,
2. broadly understood commercial trade of **lubricating oils**,
3. change of purpose and consumption of heating oil subjected to illegal decolourisation.
4. putting fuel smuggled from third countries on the market.

Intra-Community acquisition of fuel through the so-called **registered consignees** is a risk which has recently been minimised by amendments to regulations. Operating through registered consignees, entities that imported fuel for their purposes put the fuel on the Polish

market with the excise duty paid but with evaded VAT. The problem of VAT extortion is not unique to Poland. It can be observed across the European Union. According to data provided by Spain's tax service, tax shortfalls amounting to Euro 157 million were identified in 2105/2016 as a result of investigations conducted by the Spanish tax service in cooperation with other services and authorities. Annual fiscal reports published by seven other EU countries signalled problems with tax shortfalls in the trade of mineral oils. However, there may be much more such countries, as the trade of mineral oils has always been fraught with considerable risk of tax shortfalls.

In the case of heating oil, there is still the risk of decolouring and putting on the market at petrol stations. Import of fuels from third countries behind our eastern border is monitored on an on-going basis. Although fuel smuggling in fuel tanks, converted containers or canisters does not generate large tax shortfalls, it is still a threat to legal fuel distributors and it distorts fair competition.

Risks related to **lubricating oils** must be seen in two ways. Lubricating oils are products that are commonly associated with engine, hydraulic and gear oils. They are subject to the excise duty only in Poland. Laws of EU Member States are now undergoing slight changes, and some countries have taxed or introduced mixed control of these goods. Since imports of lubricating oils to Poland take place outside the EU Excise Movement Control System (EMCS) with excise duty suspended and an intention of intra-Community acquisition must be reported to the competent tax authority, importing of lubricating oil without the excise duty paid seems a relatively easy task.

The catalogue of lubricating oils includes also the so-called low-viscosity lubricating oils and low-viscosity lubricating preparations produced from diesel fuel, which makes it possible to change their purpose and use them for propulsion purposes.

In 2008, a sharp increase in the production of these oils was identified to take place under different trade names but with the identical billing composition. Since the Community customs tariff permits classification of oils with as much as 90% of diesel fuel as lubricating oils, tax warehouses released products which could almost directly, or after normal compiling, be used in combustion engines. The profile of producers of such products was also relatively simple. Put simply, they were entities which were importing diesel fuel under suspension of excise duty. Adding base oil and a small volume of lubricating additive to diesel fuel would produce a product which could be legally qualified as lubricating oil. It was sold in this form to foreign users without the excise duty. Tax warehouses which started carrying out this practice would allocate all their production output to EU markets. At first, lubricating oils from fictitious intra-Community deliveries would go to the country's petrol stations as diesel fuel. As a result of actions taken by the Customs Service, Tax Control Office and the Police, this practice evolved and unfair entities started to use triangular transactions and re-sell the goods to further EU countries, which prevented the final purchaser verification and identification of the manner of use. Actions taken by Polish and foreign customs, revenue and investigation services resulted in identification of cases of putting lubricating oils on the market as diesel fuel in Poland and other EU Member States. Since Poland had the best analytical material regarding lubricating oils, following the initiative of the Polish Customs Service, and later

also the Hungarian customs service, a working group was created in 2011 on the forum of the V4 countries to develop an analytical material for the EC to subject lubricating oils to the movement control and include them in the EMCS. This solution would enable control of lubricating oil movements in intra-Community trade.

Despite the work of the aforementioned group, the European Excise Duty Commission did not agree to subjecting these products to movement control. As a result, the problem remains unsolved on the general European market. The situation is Poland is slightly better in this respect thanks to the adopted legislative changes.

Legal regulations introduced to restrict grey economy in the trade of liquid fuels

The POPiHN has been successively increasing its forecasts regarding the grey area of fuels in our country. At first, it was around 6 – 7 percent, while in 2015 alarm bells rang because the share had grown to nearly 10%. The situation required actions to restrict the grey zone. New regulations appeared and controls at fuel entities were intensified, as were controls conducted on roads and transport controls in real time. Legislative changes, called the „fuel package", were introduced in 2016 which imposed, among others, the obligation to pay VAT at the moment of intra-Community acquisition. According to POPiHN data, the changes led to an increase in legal consumption in Poland, which meant a significant reduction of the grey zone in Poland. Based on comparison of data from the first half of 2016 and 2017, a sharp increase in the consumption of diesel fuel was noticed. Another regulation introduced was the so-called energy package – an amendment to the energy law which tidied up the market and restricted the possibility of running a fuel business only to domestic entities (either established or having a branch office in Poland). Monitoring of road transport is yet another regulation, introduced in March of this year. Under the Act of 9 March 2017 on the system of monitoring of the road carriage of goods, the obligation was imposed regarding monitoring/recording, in the electronic transport system, of goods with headings, among others, CN 2207 without excise duty marks, 2707, 2710, 2905, 2917,3403,3811,3814 including ethyl alcohol, 3824 and 3826, if the gross weight of a shipment of goods with those headings exceeds 500kg or the volume exceeds 500 litres. Under Regulation of the Minister of Development and Finance of 13 June 2017 on goods whose transport is subject to the system of monitoring of the road carriage of goods, the obligation was imposed to register transport of goods with headings CN from 1507 to 1516 and 1517, excluding margarine and liquid margarine. Regulation of the Minister of Development and Finances of 13 June 2017 on goods whose transport is subject to the system of monitoring of the road carriage of goods entered into force on 22 September 2017. Included in the monitoring system were also goods with headings from CN 1507 to 1516 and 1517, z excluding margarine and liquid margarine if the shipment's gross weight exceeds 500 kg or the volume exceeds 500 litres.

podinsp. Michał Pudło
Wydział Wywiadu Kryminalnego Zarządu CBŚP w Katowicach

Ujawnianie i zabezpieczenie mienia – praca operacyjna jako wsparcie postępowania procesowego

Streszczenie

Obecnie ocenia się, że luka podatkowa w Polsce wynosi około 80 mld zł rocznie. Jednym z najważniejszych narzędzi w walce z przestępczością jest stosowanie mechanizmów prawnych pozwalających na skuteczne pozbawianie sprawców przychodów z popełnianych przestępstw. Niemniej jednak, podkreślenia wymaga fakt, że niezwykle istotny wpływ na przebieg postępowania zabezpieczającego mają działania organów innych niż prokurator, którym powierzono prowadzenie postępowania przygotowawczego, jak np. Policja, Agencja Bezpieczeństwa Wewnętrznego czy Straży Granicznej. Rola tych organów sprowadza się m.in. do zajęcia mienia ruchomego poprzez dokonanie tymczasowego zajęcia i wskazania prokuratorowi składników mienia podejrzanego, podlegających zabezpieczeniu. Organy te, z racji przyznanych kompetencji ustawowych, poza czynnościami procesowymi mają również prawo do prowadzenia działań o charakterze operacyjno-rozpoznawczym, a problematyka zabezpieczenia majątkowego ściśle związana jest – obok instytucji tymczasowego zajęcia mienia ruchomego – również z procesem ustalenia składników majątkowych osób podejrzanych, gdzie niebagatelne znaczenie ma wynik prowadzonych czynności o charakterze operacyjno – rozpoznawczym.

Rosnąca luka podatkowa w podatku VAT, której główną przyczyną są wyłudzenia podatkowe, przybrała rozmiary i strukturę godzące w bezpieczeństwo ekonomiczne Państwa. Uszczuplenia podatkowe uderzają również w bezpieczeństwo obrotu gospodarczego poprzez naruszenie zasad uczciwej konkurencji. W konsekwencji mogą prowadzić do wyparcia z rynku uczciwych przedsiębiorców, którzy nie są w stanie sprostać konkurencji „dotowanej" przez przejęte wskutek działań przestępczych podatki. Obecnie ocenia się, że luka podatkowa w Polsce wynosi około 80 mld zł rocznie.

Jednym z najważniejszych narzędzi w walce z przestępczością jest stosowanie mechanizmów prawnych pozwalających na skuteczne pozbawianie sprawców przychodów z popełnianych przestępstw.

W literaturze przedmiotu wielokrotnie podkreśla się, że pozbawienie sprawców „owoców" popełnionego przestępstwa jest najdotkliwszą karą i stanowi efektywny sposób zwalczania zorganizowanej przestępczości. Działanie to ma na celu także pozbawienie ich możliwości prowadzenia dalszej działalności przestępczej, które wiąże się z ponoszeniem dużych nakładów finansowych. Majątek, głównie ten nielegalnie uzyskany, zwykle przenoszony jest na rzecz

zaufanych osób trzecich bądź transferowany za granicę. Działania te mają uniemożliwić przeprowadzenie zabezpieczenia majątkowego.

Jednakże, aby coś zająć, wpierw trzeba to ujawnić.

Drogi do ujawnienia majątków sprawców:

- czynności o charakterze procesowym,
- czynności o charakterze operacyjnym,
- analiza kryminalna (dla procesu jak i dla formy pracy operacyjnej, biały wywiad)

Czynności procesowe:

- przeszukania (szczegółowe),
- zatrzymania rzeczy,
- przesłuchania świadków,
- przesłuchania podejrzanych,
- oględziny,
- eksperyment.

Często od dokładnych przesłuchań, nie tylko świadków, ale i też samych podejrzanych, zależy możliwość późniejszego zabezpieczenia. Niezbędne powinny być pytania o majątek, jego składniki, ale też zadłużenie, egzekucje komornicze i wierzytelności. Często zasadnym jest dokładne ustalenie sytuacji materialnej nie tylko sprawców, ale także rodziny i znajomych.

Kolejną czynnością procesową, od której powodzenia często zależy dalsza możliwość zabezpieczenia majątkowego, jest przeszukanie. Czynność ta powinna być prowadzona wnikliwie, dokładnie, przy kontrolowaniu reakcji uczestniczących osób. Interesującym materiałem mogą być dokumenty niestanowiące wartości dowodowej dla przestępstwa stanowiącego przedmiot zainteresowania naszego śledztwa, ale które mogą ustalić składniki majątkowego podejrzanych. Przykładem mogą być faktury na remont mieszkania, domu, które tylko pozornie (formalnie) jest własnością rodziny podejrzanego, a faktycznie stanowi własność sprawcy. Podobnie będą świadczyły dokumenty stanowiące o faktycznym właścicielu środków transportu, np. mandaty za wykroczenia w ruchu drogowym.

Prawidłowym wydaje się być zapisywanie w protokole oświadczeń osób uczestniczących w czynnościach, które w pierwszej fazie trwania czynności „prawdziwie" opisują czyj dany przedmiot jest, gdzie został zakupiony i jaka jest jego wartość.

Pomoc w ujawnianiu składników majątkowych stanowią wszelkiego rodzaju bazy danych czy kanały łączności informatycznej, nie tylko do których dostęp mają służby śledcze, ale także prowadzone przez inne organy czy instytucje. Przykładem mogą być bazy prowadzone przez administrację skarbową, takie jak REMDAT, VIES, SERCE. Także wszelkiego rodzaju rejestry i kartoteki, w tym prowadzone przez podmioty prywatne.

Biały wywiad (informacje dostępne w jawnej przestrzeni, ogólnodostępnej) również może stanowić doskonałe źródło informacji, czego przykładem mogą być wszelkiego rodzaju serwisy społecznościowe.

Niezbędna jest współpraca pomiędzy służbami, a w szczególności z administracją skarbową, która z racji swych uprawnień posiada szerszy zakres do informacji finansowej niż służby, takie jak Policja. Sprawdzonym „kanałem" współpracy są wspólne grupy operacyjno-procesowe,

działanie na bazie porozumień pomiędzy odpowiednimi szefami służb czy wspólne prowadzenie powierzonych przez prokuratora śledztw.

Niebagatelną rolę dla skuteczności procedury zabezpieczenia majątkowego mają czynności o charakterze operacyjnym. W prowadzonych sprawach w stosunku do osób objętych zainteresowaniem należy dążyć również do ustalenia:

- przedmiotów użytych do popełnienia przestępstwa oraz wielkości korzyści majątkowej jaką sprawcy (sprawca) osiągnęli z popełnienia przestępstwa,
- składników majątkowych sprawców przestępstw,
- miejsca ich zbycia, ukrycia lub fikcyjnego przeniesienia na inne osoby.

Formy i metody pracy operacyjnej zgodnie z przepisami mogą i powinny służyć celom związanym z ujawnianiem przedmiotów mogących podlegać zajęciu. Dlatego czynności o tym charakterze nie można zawężać tylko i wyłącznie do ustalenia i zatrzymania sprawcy przestępstwa.

Przy transgranicznym charakterze dzisiejszej zorganizowanej przestępczości ekonomicznej, a szczególnie przestępczości „karuzelowej", niezbędnym dla realizacji zadań związanych z odzyskiem i zabezpieczeniem mienia, jest także podjecie współpracy międzynarodowej. Współpraca ta może odbywać się również na kilku kanałach, w tym o charakterze pozaprocesowym, jak za pośrednictwem Biura Międzynarodowej Współpracy Policji, Wydziału Odzyskiwania Mienia Biura Kryminalnego KGP i poprzez Europol, jak i procesowym, tak jak wnioski o międzynarodową pomoc prawną czy pomoc Eurojustu i wspólnych zespołów śledczych.

Jak ważny jest temat odzysku i zabezpieczenia mienia, stanowią zmiany w prawodawstwie, poszerzające uprawnienia służby śledczych w zakresie tej tematyki. Przykładem mogą być zmiany w ustawie o Policji dotyczące kontroli operacyjnej, gdzie dodano możliwość stosowania tego środka przy wykonywaniu czynności operacyjnorozpoznawczych, podejmowanych przez Policję w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów, ściganych z oskarżenia publicznego, umyślnych przestępstw wymienionych w katalogu, w celu ujawnienia mienia zagrożonego przepadkiem w związku z tymi przestępstwami. Możliwość tę dodano także w przepisach Kodeksu postepowania karnego, regulując „podsłuch" procesowy.

Poszerzono także dostęp dla Policji w trakcie czynności operacyjnych do informacji objętych różnego rodzaju tajemnicami, gdzie jeżeli jest to konieczne do skutecznego zapobieżenia przestępstwom, o których mowa w art. 19 ust. 1, lub ich wykrycia, ustalenia ich sprawców, uzyskania i utrwalenia dowodów, **a także wykrycia i identyfikacji przedmiotów i innych korzyści majątkowych pochodzących z tych przestępstw albo ich równowartości**, poszerzono zakres informacji dostępnych Policji, przy kontroli sądowej, co dotyczy:

- tajemnicy skarbowej,
- tajemnicy zawodowej – kasy oszczędnościowokredytowe,
- ZUS,
- funduszy inwestycyjnych,
- tajemnicy maklerskiej - instrumenty finansowe.

Jak i bez kontroli sądowej:

- dokumentacja związana z nadaniem NIP,

- tajemnica skarbowa – bez danych bankowych,
- bankowa – identyfikacja umowy (że została zawarta),
- ZUS – potwierdzenie objęcia ubezpieczeniem i dane,
- tajemnica maklerska – fakt dokonania transakcji dotyczących towarów giełdowych,
- fundusze inwestycyjne – czy jest uczestnikiem funduszu inwestycyjnego,
- tajemnica maklerska - czy jest stroną umowy dotyczącej obrotu instrumentami finansowymi,
- tajemnica ubezpieczeniowa - czy jest stroną lub innym uczestnikiem umowy ubezpieczenia.

Wskazania dla zasadności wykonywania czynności zmierzających do zabezpieczenia majątkowego pokazują aktualne Wytyczne Prokuratora Generalnego nr 5/2017 z dnia 10 sierpnia 2017 r. w sprawie zasad prowadzenia postępowań przygotowawczych w sprawach o przestępstwa związane z procederem wyłudzania nienależnego zwrotu podatku od towarów i usług (VAT) oraz innych oszukańczych uszczupleń, w tym podatku gdzie w pkt. 4 zapisano: „Już na etapie postępowania *in rem* należy podejmować – z wykorzystaniem do tego celu baz danych dostępnych prokuraturze, organom ścigania i organom finansowym – czynności zmierzające do ustalenia stanu majątkowego osób podejrzewanych o popełnienie przestępstwa oraz skutkujące dokonaniem ustaleń o rzeczach i prawach majątkowych mogących stanowić przedmiot zabezpieczenia, a znajdujących się we władaniu innych osób".

Podsumowując należy stwierdzić, że niezwykle istotny wpływ na przebieg postępowania zabezpieczającego mają działania organów innych niż prokurator, którym powierzono prowadzenie postępowania przygotowawczego, jak np. Policja, Agencja Bezpieczeństwa Wewnętrznego czy Straż Graniczna. Rola tych organów sprowadza się m.in. do zajęcia mienia ruchomego poprzez dokonanie tymczasowego zajęcia i wskazania prokuratorowi składników mienia podejrzanego podlegających zabezpieczeniu. Organy te z racji przyznanych kompetencji ustawowych poza czynnościami procesowymi mają również prawo do prowadzenia działań o charakterze operacyjno-rozpoznawczym, a problematyka zabezpieczenia majątkowego ściśle związana jest – obok instytucji tymczasowego zajęcia mienia ruchomego – również z procesem ustalenia składników majątkowych osób podejrzanych, gdzie niebagatelne znaczenie ma wynik prowadzonych czynności o charakterze operacyjno-rozpoznawczym.

Mjr. Michał Pudło

Intelligent Department Central Bureau of Investigation of the Police Regional Office in Katowice

Disclosure of and seizure of property – operational work as support of procedural acts

Abstract

At present, the tax gap in Poland is estimated to amount to around PLN 80 billion per year. One of the key tools in combating crime is application of legal mechanisms through which perpetrators can be effectively deprived of economic benefits from their criminal activities. It is often emphasised in the professional literature that deprivation of perpetrators of "the fruit" of their criminal activity is the most painful penalty and an effective method of combating organised crime.

It should be emphasised, however, that actions taken by authorities other than the prosecutor which have been assigned conduct of preparatory proceedings such as e.g. the Police, the Internal Security Agency and Border Guard play a crucial role in the course of property seizure proceedings. The role of these authorities consists in, among others, seizing movable property by means of temporary seizure and adduce, to the prosecutor, the suspected property subject to seizure. Apart from procedural activities, these authorities, based on their statutory remit, have the right to conduct operational and exploratory activities, and the subject of property seizure – together with the measure of temporary seizure of movable property – is closely linked also to the process of identification of assets of suspects, where the effects of operational and exploratory activities play a very important role.

The growing VAT gap, which is caused mainly by tax fraud, has taken on proportions that endanger the economic security of the State. Tax shortfalls endanger also the security of economic trade through violating the principles of fair competition. In consequence, they may lead to driving fair undertakings out of the market as they are unable to effectively compete with businesses „subsidised" from taxes obtained through criminal activities. At present, the tax gap in Poland is estimated to amount to around PLN 80 billion per year.

One of the key tools in combating crime is application of legal mechanisms through which perpetrators can be effectively deprived of economic benefits from their criminal activities.

It is often emphasised in the professional literature that deprivation of perpetrators of „the fruit" of their criminal activity is the most painful penalty and an effective method of combating organised crime. This action is aimed also at preventing them from continuing their criminal activities, which entails large financial costs. Property, mainly that illegally obtained, is normally assigned to trusted third parties or transferred abroad in order to avoid seizure.

However, to be seized, property must first be disclosed.

Methods of disclosing perpetrator's property:

- activities of procedural nature,
- activities of operational nature,
- criminal analysis (in procedural and operational work, white intelligence)

Procedural activities:

- search (detailed),
- seizure of goods,
- witnesses interview,
- suspect interview,
- inspection,
- experiment.

Whether property can be successfully seized very often depends on detailed interviews of not only witnesses, but also perpetrators themselves. Interview should include questions about property and components thereof, but also debts, debt enforcement procedures and receivables. It is often advisable to establish a detailed picture of the financial situation of not only the perpetrators but also their relatives and friends.

A search is another procedural activity on whose success a subsequent seizure of property is hinged. This activity should be conducted thoroughly and carefully and reactions of the participants should be observed in the process. Documents that do not have any evidence value for the crime which is the subject of the investigation concerned, but which nevertheless can be helpful in identifying the perpetrators' assets, can be an interesting material. These are, for instance, invoices for renovation of a house or flat, which is only seemingly (formally) property of the perpetrator's family but in fact belongs to the perpetrator. A similar message will be provided by documents that indicate the actual owner of means of transport, e.g. traffic tickets.

It seems appropriate to note in the record statements made by persons participating in the activities, who at first „truthfully" describe who a given item belongs to, where it was bought and what its value is.

Assistance in disclosing assets is provided by all sorts of databases and electronic communications channels that can be accesses not only by the investigating services, but other authorities or institutions. These are, for instance, databases kept by the revenue administration such as REMDAT, VIES, SERCE, as well as all sorts of registers and records, including those kept by private entities.

White intelligence (i.e. publicly available information) can be an excellent source information as well, which is demonstrated by all sorts of social media services.

Cooperation between services is necessary, particularly with the revenue administration, which, due to its remit, has a wider range of financial information than that available to services such as the Police. Proven „channels" of cooperation include joint operations and procedural teams, joint operations under agreements between heads of specific services and joint conduct of investigations assigned by the prosecutor's office.

Operational activities are extremely important for the success of the property seizure procedure. With respect to persons of interest in cases that are being conducted, investigators should strive to establish:

a) objects used to commit the crime and amounts of benefits obtained by the perpetrator (perpetrators) from the crime,
b) assets belonging to the perpetrators,
c) where these assets were sold, hidden or fictitiously transferred onto third parties.

In accordance with regulations, forms and methods of operational work can and should serve the purposes of identifying goods that may be subject to seizure. This is why these activities must not be restricted only to identifying and apprehending perpetrators.

Given the cross-border nature of modern day economic crime, particularly „carousel" fraud, tasks related to recovery and seizure of property require international cooperation as well. Such cooperation can take place through several channels, including non-procedural channels such as the International Police Cooperation Bureau of the National Police Headquarters, Asset Recovery Department at the Criminal Bureau of the National Police Headquarters and Europol, as well as procedural measures such as requests for international mutual legal assistance, Eurojust assistance and joint investigation teams.

The great importance of the subject of property recovery and seizure is evident in the light of changes in law which under which the remit of investigation services in this area has been expanded. For example, the Polish Police Act was amended in the area of operational control to permit this measure in the course of operational and exploratory activities conducted by the Police to prevent, detect, identify perpetrators as well as obtain and preserve evidence of intentional crimes prosecuted by public indictment and listed in the [Act's] catalogue in order to disclose property subject to forfeiture due to criminal activities. Such possibility was added also to the provisions of the Code of Criminal Procedure when regulating procedural „tapping".

In addition, these amendments expanded the Police access to information subject to various secrets where such access is required in the course of operational activities to effectively prevent crimes referred to in Article 19 Paragraph 1 [of the Act] or to detect, identify perpetrators, obtain and preserve evidence **as well as detect and identify objects and other material benefits from those crimes or an equivalent value thereof.** The scope of information available to the Police, subject to judicial review, includes:

- fiscal secret,
- professional secret – credit unions,
- Social Insurance Institution (ZUS),
- investment funds,
- brokerage secret – financial instruments,

Information available without judicial review:

- documentation related to assignment of a tax identification number (NIP),
- fiscal secret – excluding bank databases,
- bank secret – identification of an agreement (if concluded),
- ZUS – confirmation of insurance and related data,
- brokerage secret – fact of effecting stock exchange transactions,

- investment funds – whether a person is a member of an fund investment,
- brokerage secret – whether a person is a party to a contract on trading of financial instruments,
- insurance secret – whether a person is a party to or another participant in an insurance contract.

Recommendations regarding legitimacy of activities aimed at property seizure are set out in Guidelines No. 5/2017 of the Prosecutor General of 10 August 2017 on the rules of conducting preparatory proceedings in cases regarding crimes related to the practice of extorting undue VAT refunds and other fraudulent tax shortfalls, where it is stated in Point 4 „Already at the stage of *in rem* proceedings, initiate – with the use of databases available to the prosecutor's office, law enforcement agencies and financial authorities – activities aimed to identifying assets of suspects and leading to findings regarding goods and property rights in possession of third parties that may be subject to seizure."

Summing up, it should be said that actions taken by authorities other than the prosecutor which have been assigned conduct of preparatory proceedings such as e.g. the Police, the Internal Security Agency and Border Guard play a crucial role in the course of property seizure proceedings. The role of these authorities consists in, among others, seizing movable property by means of temporary seizure and adducing, to the prosecutor, the suspected property subject to seizure. Apart from procedural activities, these authorities, based on their statutory remit, have the right to conduct operational and exploratory activities, and the subject of property seizure – together with the measure of temporary seizure of movable property – is closely linked also to the process of identification of assets of suspects, where the effects of operational and exploratory activities play a very important role.

Arkadiusz Pytlik
Śląski Urząd Celno-Skarbowy w Katowicach

Analiza kryminalna w służbach bezpieczeństwa wewnętrznego

Streszczenie

Prezentacja przedstawia walory i uniwersalność stosowania analizy kryminalnej, jako nowoczesnego narzędzia zwalczania przestępczości zorganizowanej. Zawarto w niej krótkie omówienie historii analizy kryminalnej, procesu wdrożenia analizy kryminalnej w Służbie Celnej, definicji, statusu w procesie wykrywczym i dowodowym oraz rodzajów analizy. Przedstawione zostaną również przykłady wizualizacji wyników analizy kryminalnej w postaci: bilingów telefonicznych, przepływu towarów, przepływów finansowych, chronologii zdarzeń (wykresy z zastosowaniem osi czasu), powiązań osobowych. Omówiono ponadto procedurę zlecania wykonania analizy kryminalnej i zasady współpracy ze zleceniodawcą. Na koniec przedstawiono przykłady wykorzystania analizy kryminalnej w Służbie Celnej.

Wstęp

Zapewnienie bezpieczeństwa jest podstawową funkcją każdego państwa. Realizacja podstawowych interesów narodowych Rzeczypospolitej Polskiej to także działania służb odpowiedzialnych za bezpieczeństwo kraju. Sprawne zarządzanie bezpieczeństwem wewnętrznym to również skuteczność i efektywność działań poszczególnych służb i podmiotów. Zależeć ona może w dużej mierze od umiejętnego zarządzania informacją będącą w ich posiadaniu, a więc także od jakości czynności analitycznych. Wymogi, jakie stawia się służbom odpowiedzialnym za bezpieczeństwo państwa to sprawna wymiana informacji, dzielenie się wiedzą, kooperacja z innymi podmiotami państwowymi, ale także aktywność na arenie międzynarodowej. Czynności analityczne obejmują obszerne spektrum zagadnień, dotyczą szerokiego spojrzenia na kwestie ogólne, ale też i wąskich specjalizacji. Wykonywana współcześnie analiza informacji jest wspomagana m.in. analizą kryminalną, a ta zaznacza swą obecność w polskich służbach już od ponad 10 lat.

Analiza informacji jako metoda wykorzystywana jest w wielu dziedzinach. Jej zastosowanie w kontekście zdarzeń będących w zainteresowaniu służb państwowych, jak i innych podmiotów działających na rzecz bezpieczeństwa nie jest czymś nowatorskim. Stanowi istotny element wspomagający działania organów ścigania, pełniąc przede wszystkim rolę usługodawczą[1]. Praktycznie każdy podmiot realizujący zadania na rzecz bezpieczeństwa w swych

[1] M. Hausman, M. Kobylas, *Problemy funkcjonowania analizy kryminalnej w Polsce w kontekście aktualnych rozwiązań i doświadczeń. Sprawozdanie z III Sympozjum Analityków Kryminalnych* (Szczytno, 8-10 listopada 2004 r.), Policja 4/2004, s. 77.

działaniach stosuje analizę, ale nie każdy robi to identycznie. Elementami różnicującymi zakres jej wykorzystania są przede wszystkim obszar kompetencyjny działań oraz warsztat pracy analityka bądź osoby, która wykonuje analizy nie posiadając formalnych uprawnień. Stosowanie jednolitych technik pracy z informacjami, wykorzystanie narzędzi wspomagających procesy analityczne i przetwarzanie informacji przyczyniło się do ewoluowania analizy kryminalnej w kierunku szerszych zastosowań. Wiele podmiotów zainteresowanych rozwiązaniami policyjnymi zaadaptowało analizę kryminalną w swych działaniach, co stanowi dowód uznania jej za metodę uniwersalną.

Historia analizy kryminalnej i program Anacapa

Analizowanie jako klasyczny proces myślowy miało miejsce zawsze. Natomiast analiza w kontekście zunifikowanych technik analitycznych to element współczesny. Żeby jednak ująć w ramy czasowe początek analizy kryminalnej należy ją odpowiednio zdefiniować. *Analiza kryminalna to ustalanie i domniemywanie związków pomiędzy danymi o działalności przestępczej z innymi, potencjalnie z nimi powiązanymi informacjami, w celu ich wykorzystania przez organy ścigania i sądownictwo. Polega na identyfikacji lub możliwie dokładnym określeniu wewnętrznych powiązań pomiędzy informacjami dotyczącymi przestępstwa oraz wszelkimi innymi danymi uzyskanymi z różnych źródeł i wykorzystaniu ich do celów operacyjnych, dochodzeniowo-śledczych i strategicznych. Stanowi uznane narzędzie wspomagające procesy wykrywcze*. Analiza kryminalna jest metodą pracy Policji, która w obecnej fazie jej rozwoju na stałe zadomowiła się w realiach szeroko rozumianego procesu wykrywczego. Stanowi niejednokrotnie istotny element wspomagający działania organów ścigania, pełniąc przede wszystkim rolę usługodawczą[2].

Gwałtowny rozwój przestępczości zorganizowanej na terenie Stanów Zjednoczonych, obejmującej swoim zasięgiem obszar wielu stanów a także i obszar zagraniczny, wymusił opracowanie w latach sześćdziesiątych dwudziestego wieku, programu naukowego pod nazwą „ANACAPA", którego celem było wspomaganie działań policji. Program ten stał się punktem wyjścia dla technik i metod analitycznych stosowanych do dzisiaj w USA. Impulsem do stworzenia szeregu narzędzi związanych z wywiadem kryminalnym, w tym także programu naukowego o nazwie Anacapa przygotowanego w Stanach Zjednoczonych przez firmę Anacapa Sciences Inc., był wspomniany wcześniej rozwój przestępczości zorganizowanej. Istotnym było jednak, aby we właściwy sposób wykorzystać opracowane koncepcje analityczne i w sposób jednolity wprowadzić je w życie. Program Anacapa stał się jedną z opcji oferowaną na rynku szkoleń wywiadowczych i na gruncie europejskim szybko znalazł uznanie.

Metody i techniki analityczne oparte na rozwiązaniach amerykańskich zaczęto wprowadzać w Europie od końca lat 80. Jako pierwsi wprowadzili je Brytyjczycy, później Holendrzy. Obecnie instytucje o charakterze policyjnym każdego z państw Unii Europejskiej i Europolu pracują zgodnie z jednolitymi standardami analitycznymi. Takie rozwiązanie znacznie ułatwia współpracę policji w zwalczaniu przestępczości transgranicznej i międzynarodowej

[2] M. Hausman, M. Kobylas, *Problemy funkcjonowania analizy kryminalnej w Polsce w kontekście aktualnych rozwiązań i doświadczeń. Sprawozdanie z III Sympozjum Analityków Kryminalnych* (Szczytno, 8-10 listopada 2004 r.), Policja 4/2004, s. 77.

o charakterze zorganizowanym. Akcesja do Unii Europejskiej wymusiła przed polską policją jak i innymi instytucjami bezpieczeństwa wewnętrznego szereg nowych zadań. Jednym z nich było stworzenie odpowiednich struktur analitycznych odpowiadających standardom stosowanym w pozostałych krajach Unii Europejskiej. Budowę struktur analitycznych opartych na projekcie „ANACAPA" rozpoczęto w Polsce w 2000 roku. Pierwsze szkolenia polskich analityków prowadzili wykładowcy unijni. W oparciu o pierwszych przeszkolonych analityków rozpoczęto w Polsce tworzenie kadry naukowej oraz zaplecza dydaktycznego mogącego sprostać współczesnym wymaganiom. W początkowym okresie funkcjonował Nieetatowy Zespół ds. Szkolenia Analityków Kryminalnych w ramach Instytutu Służby Kryminalnej a następnie Zakładu Służby Kryminalnej. Istnienie grupy przedmiotowej ds. analizy kryminalnej sformalizowano 1 grudnia 2004 r. i funkcjonuje ona, do dnia dzisiejszego, w ramach Instytutu Badań nad Przestępczością Zorganizowaną i Terroryzmem Wyższej Szkoły Policji w Szczytnie[3], gdzie prowadzone są szkolenia w zakresie podstawowym jak i doskonalącym nie tylko kadr Policji ale także innych instytucji takich jak Straż Graniczna[4], Biuro Ochrony Rządu, Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Biuro Ochrony Rządu, Służba Kontrwywiadu Wojskowego, Służba Celna oraz prokuratura.

Należy podkreślić, że analiza kryminalna jest obecnie jednym ze skuteczniejszych narzędzi stosowanych w pracy policji. Ma to swoje odniesienie zarówno do pracy dochodzeniowo-śledczej, jak i operacyjnej. W analizie kryminalnej stosowane są ujednolicone techniki stawiania hipotez, rekonstrukcji przebiegu poszczególnych przestępstw kryminalnych, identyfikacji wielu innych przestępstw wykazujących związek z przestępstwami zasadniczymi, określenia struktury siatek przestępczych oraz analizy zakresu i sposobu prowadzenia działalności przestępczej[5].

Analiza, ocena i interpretacja informacji jest procesem przetwarzania informacji opartym na logicznym i kreatywnym sposobie myślenia, którego celem jest uzyskanie ustaleń (podstaw do wszczęcia dochodzeń, śledztw lub spraw operacyjnych) umożliwiających dalsze działania. Praca policyjna oparta jest w swej istocie w głównej mierze na realizacji procesów przetwarzania informacji[6].

Klasyfikacja i formy analizy kryminalnej

Podobnie jak samo pojęcie analizy kryminalnej, tak też jej klasyfikacja może być różnie prezentowana na świecie. Wspomniany wyżej brytyjski model szkolenia, w oparciu o który opracowane zostały założenia programu polskiego (zmodyfikowanego w kolejnych latach, ale z zachowaniem głównych ram szkolenia, utrzymujących jego historyczny trzon), zakładał podział analizy kryminalnej na dwa rodzaje (rysunek 1). Wyróżnione zostały: analiza operacyjna i analiza strategiczna.

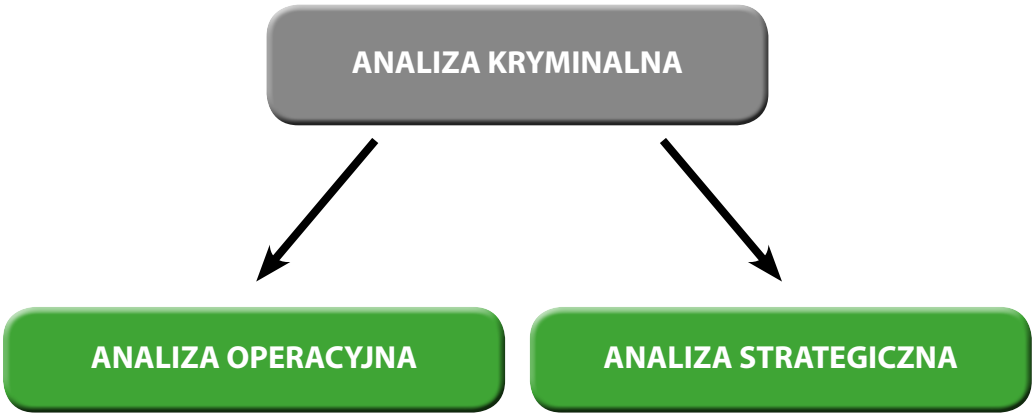
---

[3] Marcin Kobylas, Z*astosowanie analizy kryminalnej w zwalczaniu cyberterroryzmu* – referat.

[4] Od autora: po przeszkoleniu w Wyższej Szkole Policji w Szczytnie Straż Graniczna szkoli swoich analityków kryminalnych w Centralnym Ośrodku Szkolenia Straży Granicznej w Kętrzynie.

[5] Analiza kryminalna: (uaktualniona wersja 2.0.) / [przekł. Grzegorz Butrym]; Centrum Szkolenia Policji, s. 9.

[6] W. Ignaczak, *Wybrane zagadnienia analizy kryminalnej*, Szczytno, 2005 s. 9



Rys. 1. Rodzaje analizy kryminalnej (źródło: opracowanie własne)

Można spotkać się również z określeniem analiza kryminalna – ekonomiczna (finansowa)[7] służąca kompleksowemu spojrzeniu na całość informacji (zwłaszcza finansowo-księgowych) dotyczących podmiotów gospodarczych, ich interpretacji. Jej zadaniem miałoby być poszukiwanie dowodów popełnienia przestępstwa w obrocie gospodarczym. Jednakże wyodrębnianie kolejnego rodzaju wydaje się zbędne, albowiem w wyszczególnionym zakresie analizy ekonomicznej działania nie odbiegają od celów analizy operacyjnej, różnią się jedynie przedmiotem zainteresowania.

Same czynności analityczne, jak już wspomniano, mają charakter uniwersalny bez względu na to, czego dotyczą i na jakich informacjach pracuje analityk.

Analiza operacyjna

Analiza operacyjna służy osiągnięciu w krótkim czasie zamierzonego przez organy ścigania celu w postaci aresztowania sprawcy, zajęcia przedmiotu przestępstwa lub jego konfiskaty. Pojawiający się również przymiotnik „taktyczna" wynika z ujęć amerykańskich autorów, gdzie m.in. polegać ona może na takim badaniu danych, aby odpowiedzieć na pytania: gdzie, kiedy i jak dokonano przestępstwa[8]. W polskich realiach pojęcie analizy kryminalnej utożsamiane jest właśnie z analizą operacyjną[9]. Może to wynikać z faktu, iż wdrażając analizę kryminalną w Policji skupiono się głównie na wsparciu procesu wykrywczego, oczekując szybkich, doraźnych i wymiernych efektów. Również inne służby, „podglądając" te efekty, podążyły podobną drogą, zawierając w zakresie obowiązków analityków kryminalnych przede wszystkim zadania, których realizacja mieści się w zakresie analizy operacyjnej. Zaznaczyć także trzeba, iż analiza operacyjna nie obejmuje przedmiotem zainteresowania wyłącznie spraw realizowanych w ramach czynności operacyjno-rozpoznawczych. Jej spektrum obejmuje

[7] W. Ignaczak, P. Michna, *Analiza kryminalna. Zarys wykładu*, Szczytno 2002, s. 6.

[8] Chlebowicz P. i Filipkowski W., *Analiza kryminalna aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2011, s. 42

[9] W wewnętrznych przepisach policyjnych, Straży Granicznej, również korespondencji formalnej, w materiałach szkoleniowych stosowany jest też termin „operacyjna analiza kryminalna" bądź „kryminalna analiza operacyjna".

wszelkie sprawy i gromadzone w ich ramach informacje oraz wszelkie dane uzyskiwane w ramach prawnie dozwolonych metod pracy.

Cele określone w powyższej definicji analizy operacyjnej można przyjąć jako modelowe, jednakże należy takie wskazania traktować jako jedne z wielu możliwych. Niewątpliwie każda analiza operacyjna jest odmienna i odmienne też będą osiągane przez nią cele. W wieloletniej praktyce stosowania analizy kryminalnej przez polskie organy ścigania, celem takich analiz było doprowadzenie do ustalenia lub aresztowania sprawcy, zgromadzenie materiału dowodowego, nakreślenie kierunków dalszych czynności, udzielenie odpowiedzi na poszczególne zapytania wskazane przez zleceniodawcę analizy, czy „tylko" dokonanie pewnej statystyki i przedstawienie relacyjności danych (co stanowi zaledwie wycinek celów możliwych do uzyskania przez analizę operacyjną).

Podobnie jak niemożliwe jest wskazanie pełnej gamy celów analizy, tak samo wyliczanie spraw, które miałyby „trafiać" do analizy operacyjnej również jest bezcelowe. To bieżąca sytuacja weryfikuje każdą ze spraw w kontekście wystąpienia potrzeby zlecenia analizy kryminalnej. Kiedy kierować daną sprawę do analizy kryminalnej? Najwłaściwszym momentem jest subiektywne przekonanie prowadzącego sprawę o niemożności poradzenia sobie ze zgromadzonym już materiałem. Odpowiedzią formalną są wewnętrzne uregulowania prawne. Przykładem może być Zarządzenie Komendanta Głównego Policji[10] wymienia szereg okoliczności zastosowania analizy kryminalnej, wskazując następujące cechy spraw:

- wielowątkowe,
- o dużym zasięgu terytorialnym,
- w których sposób popełnienia przestępstwa wskazuje na wysoką specjalizację działalności przestępczej,
- mające rozwojowy charakter.

Każda z wyżej wymienionych cech może rodzić niejakie problemy interpretacyjne. Wielowątkowość sprawy może być odbierana liczbowo (kilka, kilkanaście), bo też ile wątków ma liczyć sprawa, by poddać ją analizie? Odpowiedź na to pytanie nie tkwi wyłącznie w określeniu minimalnej liczby całkowitej, lecz również w charakterze tych wątków. W wielu sprawach występują wątki główne, ale i uboczne, które też wymagają przeanalizowania. Niektóre wątki są mało skomplikowane, inne bardziej i czasami te właśnie elementy decydują o dalszym losie sprawy. Następna cecha to duży zasięg terytorialny. Także w tym przypadku określenie nie jest precyzyjne, albowiem „duży zasięg" może oznaczać dla jednego funkcjonariusza np. obszar wykraczający poza teren działania jego jednostki, dla innego będzie to obręb województwa itd. Kolejny element to sprawy, w których ***modus operandi*** ma wskazywać na wysoką specjalizację działalności przestępczej sprawcy bądź sprawców. Przestępcy nie legitymują się świadectwami i certyfikatami specjalizacji przestępczej (co najwyżej mogą wykorzystywać wiedzę zdobytą na uczelniach, kursach itp.). Poziom ich specjalizacji przestępczej też będzie oceniany indywidualnie przez policjanta, który sam dokonuje tej oceny przez pryzmat własnego doświadczenia zawodowego.

[10] Zarządzenie nr 1012 Komendanta Głównego Policji z dnia 23 września 2004r. w sprawie stosowania przez Policję analizy kryminalnej (Dz. U. KGP nr 20/124 2004r.), §2.

Co ciekawe, wszystkie omówione już cechy, zawarte w przywołanym paragrafie zarządzenia, powinny być spełnione łącznie. Alternatywa pojawia się w zdaniu, mówiącym o rozwojowym charakterze, który też jest mocno ocenny i niejednoznaczny. Taki charakter może przybrać każda sprawa, w przypadku której czynności śledcze rozciągają się w czasie (miesiące, lata), ale również taka, która obejmuje coraz większą liczbę powiązanych ze sobą ludzi i zdarzeń.

Można zatem przyjąć, iż twórca tych wytycznych chciał jedynie podkreślić pewną wyjątkowość analizy kryminalnej, która powinna być w Policji „zarezerwowana" głównie dla spraw „większego kalibru", priorytetowych, wielotomowych. Taka interpretacja wynika z poprzedzającego wskazywany cytat sformułowania: „w szczególności...", który oznacza, że wymienione w zarządzeniu cechy nie stanowią zbioru zamkniętego, istnieje więc możliwość rozwinięcia wachlarza zleceń na inne niż wymienione w zarządzeniu przypadki. Praktyka pokazuje, że również i takie „pomniejsze" sprawy są zlecane, oczywiście uwzględniając obciążenie pracą danej komórki analitycznej. Wydaje się zatem, że każda sprawa, co do której prowadzący jest przekonany, iż wymaga ona zlecenia analizy kryminalnej i jeżeli nie jest to błędny osąd, powinna do tej analizy mieć otwartą drogę. W innym przypadku jednostki niższego szczebla, realizujące mniej skomplikowane sprawy, mogłyby zniechęcać się bądź nawet rezygnować ze stosowania analizy kryminalnej. Wyniki badań sondażowych, między innymi dotyczące tego właśnie zagadnienia, pozwoliły ocenić czy rzeczywiście tak jest.

Wbrew opinii, że analizy wykonywane są najczęściej w sprawach o charakterze kryminalnym, w ostatnim okresie daje się zauważyć wzrost liczby zleceń w sprawach typowo gospodarczych, co wydaje się zrozumiałe z uwagi na coraz bardziej skomplikowany charakter przestępczości finansowej i rozbudowaną strukturę powiązań. O ile operacyjną analizę kryminalną wykonują wyłącznie komórki analizy kryminalnej, tyle już analizą strategiczną zajmują się komórki analityczne i inne, w zależności od celu zakresu wykonywanej analizy strategicznej.

Formy analizy operacyjnej

Elementem wspólnym poszczególnych form kryminalnej analizy operacyjnej jest prowadzenie czynności analitycznych skupionych na konkretnych sprawach w celu uzyskania doraźnych efektów, zgodnie z zakresem definicyjnym opisywanym wcześniej. Każda forma skupia wokół siebie daną technikę lub zestaw technik analitycznych, które analityk kryminalny dobiera w zależności od danej sprawy.

Kryterium klasyfikacji: przestępstwo

Analiza sprawy – polega na rekonstrukcji przebiegu przestępstwa poprzez przedstawienie chronologii zdarzeń następujących po sobie bądź występujących w tym samym czasie celem ustalenia ewentualnych zależności pomiędzy zdarzeniami, ujawnienia luk informacyjnych w zgromadzonym materiale, nieścisłości, wytyczenia kierunków dalszych czynności.

W analizie sprawy stosuje się najczęściej diagramy chronologiczne oraz inne techniki, których wybór jest zawsze indywidualny. Rekonstrukcja zdarzeń pozwala na przedstawienie w czasie danego przestępstwa, a także na uporządkowanie zgromadzonego materiału. W standardowym układzie akt spraw stosuje się kolejność wpinania kart od najstarszych dokumentów do najnowszych, przy czym decyduje o tym data wytworzenia dokumentu

lub jego wpływu do jednostki. W efekcie brak logicznego ciągu zdarzeń w zgromadzonym materiale, dokumenty, a przede wszystkim informacje w nich zawarte dotyczą różnych okresów, powodując chaos w chronologii wydarzeń. Bardzo łatwo pominąć pewne istotne fakty, nie dostrzec nieścisłości w informacjach czy opisach zdarzeń. Wizualizacja informacji w postaci diagramu chronologicznego pozwala na prześledzenie sekwencji faktów w konfrontacji z pozostałą treścią materiału, ułatwiając analityczne spojrzenie, a więc i wyciągnięcie nowych wniosków.

Analiza porównawcza spraw – prowadzona jest w celu ustalenia, na podstawie zestawionych ze sobą informacji z wytypowanych spraw, czy dane przestępstwa zostały popełnione przez tego samego sprawcę bądź sprawców. W efekcie wytypowane sprawy zostaną połączone ze sobą, a dotychczas zebrany materiał przedstawia nowe oblicze, tworząc większą grupę danych i informacji.

Sprawcy, dokonujący przestępstw seryjnych, mają niejednokrotnie powtarzalny sposób zachowań, zwielokrotniają też możliwości popełnienia błędów. Specyficzne modus operandi[11] może dotyczyć zarówno osoby, jak i grupy osób, rzadziej określonego podmiotu (firmy). Czynności analityczne, sprowadzające się do poszukiwania ewentualnej seryjności przestępstw, zmierzają do wypracowania zasad selekcji, według których można typować sprawy do dalszego porównania (na podstawie cech sprawy „A" typowane są przestępstwa podobne wyszukując inne sprawy („B", „C", „D") spośród bieżących bądź archiwalnych. Następnie ustala się kryteria, według których nastąpi właściwe porównanie, tj. zestawienie ze sobą cech opisowych i wyeksponowanie zbieżnych. Zdarzają się sytuacje, kiedy dochodzi do kilku przestępstw tego samego rodzaju i wszystkie one zostają poddane zestawieniu cech wspólnych wg zadanych kryteriów, bez wcześniejszej selekcji spraw (porwania w danym rejonie Polski, ataki hakerskie, fałszywe alarmy bombowe). Przy przestępstwach wielokrotnych należy zwrócić uwagę na wiele kryteriów, jak chociażby: cechy sprawcy (np. fizyczne, psychiczne), cechy ofiary (aspekt wiktymologiczny może okazać się niezwykle istotny, zważywszy na możliwe typowanie ofiar przez sprawcę), cechy miejsca popełnienia przestępstwa, aspekt planowania przestępstwa (przygotowanie miejsca, narzędzi, zastosowanie pułapki, technik mających na celu zmylić organy ścigania), sposób postępowania sprawcy na miejscu przestępstwa (użyte techniki, przedmioty, sposób komunikacji, zacieranie śladów, analiza semantyczna wypowiedzi) i inne w zależności od rodzaju przestępstw.

Kryterium klasyfikacji: przestępca

Analiza grup przestępczych – prowadzona jest w kierunku usystematyzowania posiadanych informacji o danej grupie przestępczej w celu przedstawienia jej struktury, określeniu, jaką rolę pełnią jej poszczególni członkowie, z uwzględnieniem istotnych dla działań grupy miejsc, obiektów (również podmiotów gospodarczych), środków transportu. Grupy mogą przybierać formę zorganizowanych lub luźno powiązanych, w których ktoś pełni daną rolę (popełnia dane przestępstwo), bez zależności w stosunku do innych członków. Analizując

[11] Jak podaje T Hanausek „jest to szczególny, charakterystyczny i z reguły powtarzalny sposób zachowania się sprawcy, w którym odbijają się indywidualne cechy, właściwości i możliwości człowieka, który ten sposób stosuje". Zob. T. Hanausek, *Kryminalistyka. Zarys wykładu*, Kraków 2000, s. 45.

grupy przestępcze zorganizowane należy brać pod uwagę uwarunkowania socjologiczne funkcjonowania jednostek w grupie formalnej i nieformalnej, których cechy również w przypadku grup przestępczych znajdują swe odzwierciedlenie. Pomimo nieformalnego charakteru przejmują one wiele zasad z funkcjonowania grup formalnych (np. militarnych, jak wojsko), gdzie przywództwo jest ściśle respektowane, a polecenia bezwzględnie wykonywane (przywódca zyskuje status, uznanie i poważanie w grupie. Zorganizowane grupy przestępcze cechują się przede wszystkim skrytością[12], stąd posiadane informacje mogą nie świadczyć wprost o strukturze i rolach jej członków, ale mogą stanowić podstawę do wnioskowania o ich charakterze.

Analiza grup przestępczych (zorganizowanych) powinna zmierzać do określenia:

- struktury hierarchicznej,
- specjalizacji i podziału funkcji członków grupy,
- antagonizmów bądź kolaboracji z innymi grupami,
- powiązań z osobami (podmiotami),
- powiązań międzynarodowych,
- zasobów (środki materialne, zaplecze logistyczne itp.).

Techniką, która przede wszystkim znajdzie zastosowanie w wizualizacji struktury grupy będzie diagram powiązań osób, obiektów, ich roli i relacji zachodzących pomiędzy nimi. Ważnym elementem takiej analizy jest umiejętność łączenia faktów, zachowań osób częstokroć w oparciu o informacje szczątkowe. Nie w każdym materiale skład grupy oraz role jej członków są rozpisane „od A do Z", a rolą analityka jest tylko usystematyzowanie tej wiedzy, zakładając, że takie zadanie w ogóle zostanie mu zlecone. Czasem na pozór oczywista sieć powiązań, po wnikliwej analizie zebranego materiału, okazuje się bardziej skomplikowana. Wiele zależy od tzw. „czytania między wierszami", ważnej umiejętności analityka, który oprócz klasycznego zestawiania faktów musi odnieść się do swojej intuicji, doświadczenia czy też samodzielnego pogłębiania informacji (np. w otwartych źródłach informacji).

Analiza profilu szczególnego – jest to próba określenia na podstawie opisu przestępstwa cech charakterologicznych osoby, która je popełniła[13]. Sporządzenie charakterystyki cech psychologicznych sprawcy wymaga udziału eksperta – psychologa. Nie jest to powszechnie stosowana praktyka w pracy polskich organów ścigania, niemniej można już mówić o wzroście zainteresowania tą „usługą" w Policji, zwłaszcza w przypadku groźnych, brutalnych przestępstw (np. zabójstw, zgwałceń, podpaleń, aktów terrorystycznych[14]). Współcześnie należy powiązać przedstawione zagadnienie z pojęciem profilowania kryminalnego, pomimo szerszego spektrum zainteresowań tego drugiego. Zakres analizy profilu szczególnego istotnie koresponduje ze stanowiskiem agentów FBI – pionierów profilowania, którzy definiują je jako określenie cech sprawcy opierające się na analizie popełnionego przestępstwa, którego wynikiem jest

[12] B. Hołyst, E. Kube, R. Schulte, *Przestępczość zorganizowana w Niemczech i w Polsce. Zwalczanie i zapobieganie,* Warszawa 1998, s. 51.

[13] Analiza kryminalna (uaktualniona wersja 2.0.),op. cit., s. 29.

[14] Więcej: K. Liedel, *Profilowanie sprawców przestępstw terrorystycznych*, [w:] J. Konieczny, M. Szostak (red.), tamże, s. 186-203.

ogólna charakterystyka osoby[15]. Specjalistów, sporządzających charakterystyki psychologiczne nieznanych osób nazywa się profilerami. W swoich charakterystykach, mimo własnych doświadczeń w sprawach kryminalnych, zdecydowanie bardziej opierają się na naukowych podstawach profilowania (kryminalnego – w przypadku sprawców przestępstw). Ekspercki charakter profilowania kryminalnego wiąże się z koniecznością zgłębiania m. in. psychologii, kryminalistyki, kryminologii, wiktymologii, psychiatrii, medycyny sądowej, socjologii, seksuologii czy nawet statystyki[16]. Multidyscyplinarny charakter profilowania kryminalnego przeplata się z wiedzą praktyczną i intuicją profilera. Profilowanie kryminalne, zmierzając do nakreślenia cech osobowościowych, fizycznych, społecznych i innych w zależności od konkretnego przypadku, skupia się na relacjach łączących sprawcę i ofiarę, miejscu popełnienia przestępstwa, czy ustaleniu motywu[17], niezwykle istotnego dla późniejszych czynności wykrywczych (motyw działania sprawcy może być nieznany, sprawca może też kierować uwagę organów ścigania na fałszywy motyw).

Analiza profilu szczególnego, zgodnie z przyjętym wcześniej założeniem, mieści się w zakresie profilowania kryminalnego (które jest pojęciem znacznie szerszym), te zaś, zachowując zasady przypisane analizie kryminalnej, zwłaszcza w sferze wnioskowania analitycznego, powinno opierać się na przesłankach dających się należycie uzasadnić. Profil kryminalny może być wykorzystywany również w kształtowaniu dalszych czynności wykrywczych nie tylko do typowania sprawców i weryfikacji podejrzewanych osób, ale też do przygotowania się do czynności procesowych (przesłuchanie – treść pytań, przeszukanie – lista rzeczy itp.), określenia kierunku gromadzenia dalszych informacji.

Kryterium klasyfikacji: metody kontrolne

Analiza prowadzenia sprawy – jest to ocena dotychczasowych działań i metod zastosowanych w realizowanej sprawie w celu określenia ich dalszego przebiegu. Forma ta zmierza do badania przebiegu czynności i zastosowanych w sprawie metod, a w ich ramach – efektywności uzyskiwania informacji[18]. Obejmuje sprawy priorytetowe dotyczące poważnych przestępstw, do prowadzenia których została powołana zazwyczaj grupa dochodzeniowo-śledcza. W takich przypadkach w ciągu kilku czy kilkunastu miesięcy prowadzenia sprawy dochodzi do starcia się koncepcji osób prowadzących, zastosowane metody przynoszą różne efekty w korelacji z czasem, przyjęte wersje tracą i zyskują na znaczeniu podczas ich weryfikacji. W wyniku interakcji zachodzącej w grupie osób prowadzących sprawę może dojść do bezkrytycznego przyjęcia przez grupę jednego kierunku działań (jednej zakładanej wersji), kurczowego trzymania się wybranych działań, co z kolei doprowadzić może do wyczerpania się ich „arsenału". Sprawy takie zatrzymują się w miejscu, wręcz wymagają świeżego spojrzenia osoby z zewnątrz, niezwiązanej ze sprawą, a taką osobą z pewnością będzie analityk kryminalny. Taka

[15] R.K. Ressler, J.E. Douglas, A.G. Burgess, R.L. Depue, Violent Crime, FBI Law Enforcement Bulletin 54 no. 8, 1985, [cyt. za:] J. Gołębiowski, *Profilowanie kryminalne*, Warszawa 2008, s. 8.

[16] Więcej: A. Huzior-Kamińska, *Medycyna sądowa w służbie profilowania kryminalnego sprawców zabójstw*, [w:] J. Konieczny, M. Szostak (red.)..., op. cit., s. 80-98.

[17] J. Gołębiowski, *Profilowanie kryminalne*, Warszawa 2008, s. 10.

[18] Analiza kryminalna (uaktualniona wersja 2.0.), op. cit., s. 34-35.

analiza rzadko występuje jako niezależna forma, najczęściej jej elementy pojawiać się będą przy okazji innych obranych kierunków czynności analitycznych. Dotychczas zaprezentowane formy analizy operacyjnej, jak już zasygnalizowano, nie poddają się analogicznemu wyodrębnieniu w praktyce, czynności analityczne stale się przenikają i uzupełniają w ramach zleconej analizy kryminalnej, rzadko pozostając w pierwotnej formie zgodnej z opisaną klasyfikacją.

Analiza strategiczna

Eksperci Interpolu wskazują, że przedmiotem analizy strategicznej są problemy i cele długoterminowe, ustalenie priorytetów i strategii zwalczania przestępczości kryminalnej na podstawie dogłębnych badań oraz prognozowanie jej rozwoju"[19]. W służbach bezpieczeństwa publicznego analiza strategiczna znajduje zastosowanie w identyfikowaniu i rozwiązywaniu problemów dotyczących przestępczości.

Analiza strategiczna obejmuje swym zakresem przede wszystkim:

- monitorowanie ogólnej sytuacji w kraju,
- monitoring poszczególnych sektorów przestępczości,
- wykrywanie nowych trendów przestępczości,
- duże organizacje przestępcze,
- analizę metod dochodzeniowych,
- studium zapobiegania zachowaniom przestępczym,
- ogólną statystykę przestępczości,
- ewolucję skuteczności działań związanych z bezpieczeństwem,

Analizy strategiczne dotyczące konkretnej przestępczości, powinny uwzględniać informacje i dane obiektywne, współwystępujące, jak np. dane demograficzne, zagospodarowanie terenu, dane geograficzne – zwłaszcza powiązane z Systemem Informacji Geograficznej (GIS)[20], meteorologiczne, archiwalne, faktograficzne, regulacje prawne, procedury etc. Niektóre analizy strategiczne mogą wymagać udziału bądź wsparcia ekspertów z różnych dziedzin (m.in. statystyków, prawników, ekonomistów, psychologów), mogą przybierać postać obszernych raportów jednorazowych bądź cyklicznych. Analizy strategiczne służą podejmowaniu decyzji w sprawach bieżących danego podmiotu, w sytuacjach nietypowych, nadzwyczajnych, ale też w kontekście działań i planów długofalowych, strategii podmiotu.

W przeciwieństwie do operacyjnej analizy kryminalnej oscylującej na ogół wokół pojedynczej sprawy, kryminalna analiza strategiczna odnosi się do liczby mnogiej przestępstw, spraw, zjawisk. Również okres, który obejmuje, zazwyczaj jest zdecydowanie szerszy niż ma to miejsce w przypadku analizy operacyjnej. W analizach strategicznych prezentowane są często uogólnienia, zestawienia zbiorcze, trendy, wzorce i odstępstwa od nich, wskaźniki wzrostu i spadku przestępczości, cech zjawiska itd. W praktyce wykonywana jest przez analityków kryminalnych dużo rzadziej niż analiza operacyjna. Finalnie przybiera często postać raportu, opisu statystycznego, tabel, a także analizy geograficznej.

[19] Analiza kryminalna (uaktualniona wersja 2.0.), op. cit., s. 16.

[20] GIS – ang. Geographic Information System.

Formy analizy strategicznej

Poszczególne formy analizy strategicznej zaprezentowane poniżej bardziej skupiają się na opisie tego, czego dotyczą, niż na sposobach wykonania, pozostawiając miejsce na autorski dobór technik pracy, które na bieżąco będą wspierane nowymi narzędziami informatycznymi i osiągnięciami nauki.

Kryterium klasyfikacji: przestępstwo

Analiza przestępczości – skupiona jest wokół powziętego do analizy rodzaju przestępczości (wg kategorii, typu, artykułu kodeksu karnego, innych), a konkretnie jej przejawów na danym terenie i w danym czasie. Ujęcie fenomenologiczne pozwoli na wskazanie pewnych trendów przestępczości, cech szczególnych, prognoz co do dalszego ich rozwoju, planów strategii działań jednostki. Zaprezentowane w raportach: tabele, wykresy, diagramy, opisy statystyczne coraz częściej uzupełniane są wynikami analiz geoprzestrzennych z zastosowaniem systemu GIS[21] (w instytucjach bezpieczeństwa wewnętrznego takich jak Policja, Krajowa Administracja Skarbowa wykorzystywane jest oprogramowanie ArcGIS[22]), w których aspekt wykorzystania mapy znacznie wykracza poza tradycyjne naniesienie ognisk, punktów przestępczości.

Kryterium klasyfikacji: przestępca

Analiza profilu ogólnego – polega na ustaleniu cech opisujących sprawców przestępstw danego rodzaju, które się powtarzają lub są podobne w zestawionych dotychczasowych przypadkach.

Analiza profilu ogólnego może znaleźć szerokie zastosowanie, m.in. w sytuacjach, które wymagają komunikacji ze społeczeństwem (ostrzeżenie przed sprawcami i metodami działania np. oszustwa metodą „na wnuczka"), wymagają szybkiej reakcji służb państwowych (groźby zamachów terrorystycznych, uprowadzenia osób), przyśpieszą selekcje osób podejrzewanych i typowanie sprawców (np. w przypadkach wykorzystania seksualnego dzieci). Sporządzona charakterystyka osób (sylwetka sprawcy przestępstwa danego rodzaju) może stanowić podstawę weryfikacji dotychczasowych czynności, punkt odniesienia do dalszych działań, swoistą matrycę kontrolną.

W analizie profilu ogólnego wykorzystuje się m.in. narzędzia statystyczne, przestrzenne odniesienia (zwłaszcza z wykorzystaniem GIS), analizy porównawcze, zestawienia tabelaryczne.

Kryterium klasyfikacji: metody kontrolne

Analiza metod stosowanych w sprawach – prowadzona jest w celu udoskonalenia warsztatu pracy osób odpowiedzialnych za wykonywanie określonego typu spraw.

Pomimo narzuconego odgórnie (przepisy, dyspozycje przełożonego) katalogu działań wynikających ze specyfiki analizowanego zagadnienia, zawsze występują pewne odmienności.

[21] System GIS to oprogramowanie służące do obsługi map cyfrowych.

[22] Oprogramowanie ArcGIS składa się z wielu elementów z rozbudowanymi funkcjonalnościami edycji, analizy i prezentacji kartograficznej, zarządzania danymi

Dotyczyć one mogą doboru sposobów działania, zastosowanych środków, kolejności czynności, skupienia szczególnej uwagi na danych zagadnieniach itd. W efekcie stopień skuteczności pewnych czynności różni się w poszczególnych jednostkach. Omawiana forma analizy ma na celu ustalenie, które z przyjętych metod miały realny wpływ na korzystny wynik prowadzonych spraw, rozpatrując słabe i mocne strony działań. Należy w przedmiotowej analizie uwzględniać i porównywać czynniki zakłócające obiektywny obraz rzeczywistości, mogą to być np. specyfika danego terenu i charakterystycznej dla niego przestępczości (przemyt w rejonach przygranicznych), obciążenia sprawami pracowników wykonujących czynności (liczba osób w danej komórce, wakaty, absencje), poziom przeszkolenia kadry, wyposażenie w środki niezbędne do prowadzenia czynności (środki finansowe, łączność, logistyka...). Wyniki przeprowadzonej analizy metod stosowanych w sprawach mogą znaleźć zastosowanie w szkoleniach, instruktażach, wytycznych, okólnikach, specjalistycznych raportach. Mogą także stanowić przesłankę do zmian organizacyjnych w danej jednostce.

Omawiane formy analizy operacyjnej i strategicznej mają niewątpliwie charakter uniwersalny, który wiązać się może z ich stosowaniem w zwalczaniu wszelkich przejawów przestępczości, ale również w pozostałych działaniach podejmowanych przez służby i podmioty państwowe.

W ramach poszczególnych form analizy kryminalnej stosowane są konkretne sposoby działań, które indywidualnie dobierane przez analityka są pomocne w osiąganiu zakładanych przez analizę celów.

Zaznaczyć należy, że poszczególne formy zbyt sztywno przewidują niektóre zakresy czynności analitycznych. Wynika to zapewne bardziej z próby systematyzacji wykonywanych analiz niż z praktycznego ujęcia zagadnienia, szczególnie w stosunku do form analizy operacyjnej, które w praktyce ich stosowania wzajemnie się przenikają i uzupełniają. Potwierdzeniem tego są doświadczenia i wnioski płynące z przeprowadzanych dotychczas kryminalnych analiz operacyjnych w Polsce. Jednakże warto zapoznać się z poszczególnymi formami znajdującymi zastosowanie na świecie i w Polsce z uwagi na zakres czynności analitycznych, jaki obejmują. Rozwijają też szczegółowo dotychczasowe ujęcie definicyjne analizy kryminalnej i jej rodzajów. Poszczególne formy analiz: operacyjnej i strategicznej, zostały omówione według trzech kryteriów: przestępstwo, przestępca, metody kontrolne.

Rodzaje analiz		Analiza operacyjna	Analiza strategiczna
Kryterium	Przestępstwo	Analiza sprawy	Analiza przestępczości
		Analiza porównawcza spraw	
	Przestępca	Analiza grup przestępczych	Analiza profilu ogólnego
		Analiza profilu szczególnego	
	Metody kontrolne	Analiza prowadzenia sprawy	Analiza metod stosowanych w sprawach

Tab. 1. Formy analizy operacyjnej i strategicznej (źródło: opracowanie własne na podstawie materiałów szkoleniowych WSPol w Szczytnie)

Rola informacji i jej źródła w analizie kryminalnej

Współczesne zarządzanie informacją staje się domeną już nie tylko służb państwowych, ale także podmiotów i osób prywatnych. Wzrost liczby źródeł uzyskania informacji, możliwości magazynowania oraz jakości przetwarzania sprawia, iż dzisiejsza analiza staje się procesem bardziej efektywnym i znacznie szybszym.

Analiza kryminalna, która bazuje na dużej liczbie danych i informacji, zdecydowanie musi nadążać za ogólnym trendem w dzisiejszej analizie informacji. Należy zatem prześledzić proces uzyskiwania informacji i sposoby jej oceniania, zanim zostanie logicznie przetworzona i przejdzie na „wyższy poziom" w procesie analizowania – przekładając się na późniejsze wnioski.

Analiza informacji kryminalnych

Często w potocznym ujmowaniu zagadnienia stawia się bezwiednie znak równości pomiędzy określeniami: „dane" i „informacje", podczas gdy pojęcia te nie są synonimami. Dane od informacji należy odróżniać, gdyż dane są pierwotne w stosunku do informacji, które są wynikiem przetwarzania danych. Zatem używanie terminu „przetwarzanie" informacji może wręcz rodzić konotacje negatywne i kojarzyć się z manipulowaniem informacjami. Niemniej w procesie analitycznym możliwe jest stosowanie pojęcia „przetwarzanie informacji", rozumianego jako proces konstytuowania się wiedzy danego podmiotu na bazie uzyskanych i merytorycznie zestawionych ze sobą informacji, które tworzą logiczną całość, a następnie stanowią podwaliny pod procesy decyzyjne. Na bazie powyższych rozważań można wyraźnie wskazać na rozgraniczenie pojęć: dane, informacja, wiedza. Dane przyjmują najczęściej postać nieustrukturyzowanych faktów gromadzonych, czy to w wyniku obserwacji (treści rozmów, liczba spotkań określonych osób, liczba dostaw i ich charakter etc.), czy też poprzez zapis na określonych nośnikach (np. dane o połączeniach telefonicznych, dane o ruchu sieciowym numeru IP komputera, dane o przelewach finansowych na rachunkach bankowych wiadomości e-mail, etc.). Sposób i źródło generowania danych sprawia, że mają one zdecydowanie obiektywny charakter. Dane wymagają przetworzenia ich przez człowieka, by zyskały miano informacji. Od subiektywnej oceny i interpretacji danych zależy późniejszy kształt informacji, tak więc każdy może przedstawić różniące się treści informacji na bazie tych samych danych.

Informacja jest wynikiem przetworzenia szeregu danych i przy założeniu, że jest ona efektem procesu myślowego, staje się jasnym i celowym komunikatem twórcy informacji, więc jest wtórna w stosunku do danych, a ponadto zabarwiona subiektywnie.

Na pojęcie „informacja kryminalna" można natknąć się w zapisach ustawowych (Ustawa o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych[23]). Ustawodawca, nie wdając się w szczegóły terminologiczne, szeroko definiuje to pojęcie określając, że: „informacje kryminalne – to określone w art. 13 ust. 1 [określa szczegółowo zakres gromadzonych informacji kryminalnych – przyp. autora] dane dotyczące spraw będących przedmiotem czynności operacyjno-rozpoznawczych, wszczętego lub zakończonego postępowania karnego,

[23] Ustawa z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych, z późn. zm. Dz.U. 2010 nr 29 poz. 153.

w tym postępowania w sprawach o przestępstwa skarbowe oraz dotyczące innych postępowań lub czynności prowadzonych na podstawie ustaw przez podmioty określone w art. 19 i 20 [artykuły te wyliczają podmioty uprawnione do otrzymywania i podmioty zobowiązane do przekazywania informacji kryminalnych do Krajowego Centrum Informacji Kryminalnych – przyp. autora], istotnych z punktu widzenia czynności operacyjno-rozpoznawczych lub postępowania karnego"[24]. Zbierane, a następnie gromadzone, przetwarzane i przekazywane przez Komendanta Głównego Policji (podmiot zobowiązany zgodnie z zapisami cytowanej ustawy) informacje kryminalne stanowią de facto zbiór danych i informacji, które w wyniku dalszej analizy stają się wiedzą określonego podmiotu. Informacja (również będąca w zainteresowaniu analityka kryminalnego) powinna charakteryzować się pewnymi cechami[25]:

- użycie informacji nie powoduje jej zniszczenia, a przy powielaniu i przenoszeniu nie jest zużywana,
- może być akumulowana w bardzo długim czasie,
- nie jest w pełni podzielna: jej część może nie stanowić żadnej informacji,
- zbiór informacji jest niewyczerpany,
- jest dobrem nieprzywłaszczalnym: replika nie różni się niczym od wzorca i ma tę samą wartość,
- informacja ważna dla jednych podmiotów może okazać się bezużyteczna dla innych,
- wartość informacji zależy od momentu jej użycia (to, co miało wartość wczoraj, dziś może być już bezużyteczne).

Są to cechy niezwykle uniwersalne, lokalizujące informację (i jej znaczenie) w każdej dziedzinie życia, a więc również w kontekście bezpieczeństwa państwa stanowią wartościujące repertorium.

Wiedzę określa się m.in., jako zasób informacji z jakiejś dziedziny. Można przyjąć, iż suma wiedzy, którą posiadają poszczególne osoby, tworzące daną organizację czy też podmiot, stanowi „wiedzę podmiotu". Liczba informacji nie zawsze jednak przekłada się na jakość wiedzy, zaś jakość informacji decyduje o tym, czy wiedza zostanie wzbogacona. Często w procesie wywiadowczym dochodzi do sytuacji, że uzyskiwane są informacje, których jakość i wartość pozostawiają wiele do życzenia. Wzbogacają one oczywiście ilościowo zasób informacyjny danego podmiotu, jednakże nie zyskuje na tym jego wiedza.

Człowiek stanowi niezwykle cenne (niekiedy jedyne) źródło informacji, jednakże nie sposób nie zauważyć informacji w postaci innych źródeł. Ich liczba, dostępność i łatwość gromadzenia wpływa na zwiększenie potencjału analitycznego. Każdorazowo mówiąc o analizie informacji kryminalnej należy odnieść się do zasobów, z których zostały one zaczerpnięte.

Źródła informacji w analizie kryminalnej

Akta sprawy (materiał) dostarczone wraz ze zleceniem analizy kryminalnej stanowią główny zasób danych i informacji. Jednak również bazy danych (wewnętrzne, zewnętrzne), archiwa, rejestry czy inne źródła (zamknięte, otwarte) dysponują zasobami informacyjnymi będącymi

[24] Tamże.

[25] M. Olender-Skorek, K.B. Wydro, *Wartość Informacji*, Telekomunikacja i Techniki Informacyjne, tom nr 1-2/2007, Warszawa 2007, s. 72.

w zainteresowaniu analityka kryminalnego. Dlatego też dane i informacja stanowią punkt wyjścia pracy analityka, a ich brak sprawia, iż każda analiza ubożeje, proporcjonalnie do tych braków. System Informacji Operacyjnej stanowi bogatą i istotną bazę danych dla każdego funkcjonariusza Policji poszukującego kierunkowych informacji, tym bardziej dla analityka kryminalnego. Nie jest to jednak wyłączne źródło bazodanowe, z którego w trakcie wykonywanych analiz można i należy korzystać (oczywiście uwzględniając każdorazowo zasadność wglądu do bazy). Również inne zbiory stanowią wartościowe źródło danych i informacji. Mają one istotne znaczenie w procesie analizy, nie tylko w aspekcie zbierania i wiązania informacji, ale też weryfikacji przyjmowanych założeń i hipotez.

W zależności od zapotrzebowania oraz charakteru prowadzonych analiz kryminalnych w Policji (również zależnie od kreatywności samego analityka kryminalnego), proces analizy kryminalnej prowadzony może być w oparciu o różne bazy, w Policji są to:

- System Informacji Operacyjnej (SIO),
- Krajowy System Informacyjny Policji (KSIP),
- Automatyczny System Identyfikacji Daktyloskopijnej (AFIS),
- Policyjny Rejestr Imprez Masowych (PRIM),
- System Ewidencji Wypadków i Kolizji (SEWiK),
- rejestr „Broń",
- Krajowe Centrum Informacji Kryminalnych (KCIK),
- Centralna Ewidencja Pojazdów i Kierujących (CEPIK),
- Centralna Ewidencja Ludności (CEL), w tym: Powszechny Elektroniczny System Ewidencji Ludności (PESEL) oraz zbiory meldunkowe,
- Centralna Ewidencja Wydanych i Unieważnionych Paszportów,
- krajowy zbiór rejestrów, ewidencji i wykazu w sprawach cudzoziemców o nazwie „System Pobyt",
- Wizowy System Informacyjny (VIS),
- Krajowy Rejestr Karny (KRK),
- Kartoteka Skazanych i Tymczasowo Aresztowanych (KSiTA),
- Centralna Baza Danych Osób Pozbawionych Wolności Noe.NET,
- Zintegrowany System Ewidencji Straży Granicznej,
- Krajowy Rejestr Sądowy (KRS),
- Ewidencja Działalności Gospodarczej (EDG),
- Rejestr Zastawów (RZ),
- Nowa Księga Wieczysta (NKW),
- Krajowy Rejestr Urzędowy Podmiotów Gospodarki Narodowej (REGON),
- szeroko pojmowane źródła (częściowo już wymienione) wykorzystywane podczas śledztwa finansowego oraz ujęte w ESOM (Elektroniczny System Odzyskiwania Mienia),
- Baza Danych Obiektów Topograficznych (BDOT10k)[26],

[26] Powstała w wyniku realizacji przez Główny Urząd Geodezji i Kartografii projektu Georefernycjna Baza Danych Obiektów Topograficznych (GBDOT), pozwoli na udostępnianie zasobów danych topograficznych i geograficznych gromadzonych przez polską Służbę Geodezyjną i Kartograficzną instytucjom publicznym i podmiotom gospodarczym, które wykorzystują systemy geoinformacyjne przy realizacji własnych zadań oraz celem wspierania procesów

- międzynarodowe bazy danych.
- inne źródła, takie jak: internetowe strony rządowe: GEOPORTAL i GEPORTAL 2, informacje anonimowe, opinie prywatne (specjalistów, biegłych)199, pozostałe źródła jawne, na podstawie których prowadzony jest wywiad jawno-źródłowy (OSINT[27]).

Eksploracja takiego potencjału baz danych oraz źródeł informacji (uwzględniając fakt, że nie jest to katalog zamknięty) wskazuje na różnorodność możliwych do uzyskania informacji i danych, a w konsekwencji zdobytej wiedzy, którą może i powinien posiąść analityk kryminalny. Mnogość źródeł informacji decyduje o jakości „wiedzy kryminalnej", co sprawia, że ograniczanie się analityka kryminalnego wyłącznie do materiałów przekazywanych wraz z wnioskiem o wykonanie analizy kryminalnej jest mało efektywne, a czasami wręcz nieprofesjonalne. W aspekcie działalności wywiadowczej, zarządzanie informacją uzyskaną i następnie zmagazynowaną w bazach danych wymaga jej weryfikacji i właściwego wykorzystania. Tym samym nie może ona jedynie zaistnieć w bazie, lecz jej uzyskanie w poczet wiedzy podmiotu wymusza dynamikę i dalsze działania reaktywne, a tu silnie eksponowany jest już proces analityczny. Dbałość o jakość i liczbę informacji staje się immamentną cechą każdego działania wywiadowczego, a więc i procesu analitycznego. Sama jednak liczba i jakość informacji zawsze była związana z oceną jej samej, jak i źródła, z którego pochodzi. Tylko jednolity sposób oceny informacji oraz jego źródła zapewnić może przejrzysty sposób gromadzenia i przetwarzania już ocenionych informacji, a co za tym idzie możliwość trafnego, przemyślanego i bezpiecznego podejmowania decyzji.

System oceny informacji i ich źródeł (4x4)

Każda formacja państwowa zbierając informacje, dąży do ich weryfikacji i wykorzystania. Jednakże czynności te wymagają czasu, a okoliczności sprawy niejednokrotnie wymuszają niejako ocenę adhoc zdobytej informacji. Sama ocena wstępna jakiejkolwiek uzyskanej informacji dokonywana jest przez twórcę dokumentu, ale też każdy, kto ten dokument ma możliwość służbowo wykorzystać również dokonuje własnej interpretacji oraz oceny jakości i wiarygodności danej informacji. System oceniania informacji, stosowany przez wiele lat przez polskie służby (zarówno PRL jak i RP) daleki był od ideału, zaś sposób dystrybucji uzyskanej wiedzy sprowadzał się głównie do dekretowania dokumentacji tradycyjnej i jej przekazu wytypowanej komórce. Pogłębienie przekazanej przez innego funkcjonariusza (często z innej komórki) informacji, zwłaszcza w kontekście oceny jej wiarygodności przez autora dokumentu, sprowadzało się do konieczności bezpośredniego bądź pośredniego kontaktu z tą osobą, co nie zawsze było możliwe. W późniejszym czasie, wraz z rozwojem technologii informatycznych, część danych trafiała do systemów bazodanowych, jednakże sporo cennej wiedzy zostawało w szafach lub też nie była nawet przelewana na papier i „pozostawała

decyzyjnych dostępnych także przez portal www.geoportal.gov.pl, przy wykorzystaniu klasycznych narzędzi informatycznych GIS, źródło: strona internetowa Głównego Urzędu Geodezji i Kartografii http://www.gugik.gov.pl/projekty/gbdot, stan z dnia 14 stycznia 2014 r.

[27] Ang. Open Source Intelligence, więcej na ten temat: K. Radwaniak, P. J. Wrzosek, *Biały wywiad w Policji – pozyskiwanie i analiza informacji ze źródeł otwartych*, [w:] J. Konieczny (red.), *Analiza informacji...,* op. cit., s. 109-150.

w głowach" funkcjonariuszy. Taka sytuacja rodziła swoiste „prywatyzowanie" uzyskiwanych informacji bądź ograniczone, najczęściej lokalne jej wykorzystanie. W tej sytuacji koniecznością było przeprowadzenie zmian w zakresie zarządzania informacją, zwłaszcza w kontekście jej oceniania i dalszej eksploatacji.

W celu uzyskania jednolitego sposobu przetwarzania i interpretacji informacji oraz jej oceny i źródła, od którego pochodzi, wprowadzono w polskiej Policji a także i innych służbach bezpieczeństwa wewnętrznego system oceny informacji „4x4 "[28]. Nazwa ta wskazuje na iloczyn kodów oceny wiarygodności – czterech nadawanych źródłu oraz czterech przypisywanych samej informacji od tego źródła. System ten wprowadził zindywidualizowany sposób oceny każdej z osobna informacji.

Nadawanie kodów dla źródła i osobno dla informacji ma na celu efektywną ocenę tych dwóch elementów z zachowaniem jednorodności systemu oceniania w całej organizacji jaką jest Policja (w późniejszym czasie inne służby). W efekcie uzyskuje się kompleksowo oceniony meldunek informacyjny, który można w każdej chwili (po spełnieniu wewnętrznych uregulowań) wykorzystać. Przyśpieszenie procesu decyzyjnego sprowadza się także do zasad interpretacji zakodowanych meldunków, które w momencie nadawania kodów 4x4 i w chwili ich odczytu mają zunifikowany charakter.

Przyjmowane w minionej dekadzie opisy poszczególnych kodów ulegały nieznacznym modyfikacjom, jednakże nie wpłynęły one na sens poszczególnych kodów oceny źródła czy oceny informacji. Obecnie stosuje się następujące zestawy kodów oceny:

- dla źródła

1) kod „A" – brak wątpliwości co do wiarygodności źródła informacji,
2) kod „B" – informacja pochodzi ze źródła, które w większości przypadków dotychczas było wiarygodne,
3) kod „C" – informacja pochodzi ze źródła, które w większości przypadków dotychczas nie było wiarygodne,
4) kod „X" – informacja pochodzi z nowego źródła, którego wiarygodność nie jest znana, bo źródło nie było sprawdzane lub sprawdzenie nie jest możliwe.

- dla informacji

1) kod „1" – informacja jest oceniana jako prawdziwa przez funkcjonariusza,
2) kod „2" – fakty wskazane w informacji są znane bezpośrednio źródłu przekazującemu informację,
3) kod„ 3" – fakty wskazane w informacji nie są znane bezpośrednio źródłu przekazującemu informację, ale zostały potwierdzone przez inne źródła informacji,
4) kod„ 4" – fakty wskazane w informacji nie są znane bezpośrednio źródłu przekazującemu informację i nie mogą być sprawdzone przez inne aktualnie dostępne źródła informacji.

Źródła, oznaczone kodami A lub B, uznawane są za wiarygodne, jednakże samo wejście w posiadanie informacji przez te źródła może mieć charakter bezpośredni bądź pośredni.

[28] System stosowany także w Europolu i wielu państwach UE.

Informacja może też być na daną chwilę możliwa lub niemożliwa do weryfikacji (chociażby w częściowym zakresie). W związku z tym wiarygodne są wyłącznie te meldunki informacyjne, które zostały opatrzone jedną z następujących par kodów A1, A2, B1, B2. Pozostałe kombinacje kodów (A3, A4, B3, B4, C1-4, X1-4) sytuują meldunki w kategorii niewiarygodne, lecz nie oznacza to informacji nieprawdziwych. Są one zasobem informacyjnym organizacji (w opisywanym przypadku Policji), jednakże wymagającym przeprowadzenia dalszych czynności w celu potwierdzenia ich treści, a więc ich rzetelnej weryfikacji.

Całościowy system oceniania źródeł i informacji oraz ich ochrony stanowi kompleksowe rozwiązanie wspierające w istotny sposób filary wywiadu kryminalnego. Jest to jednocześnie rozwiązanie uniwersalne, które z powodzeniem może znaleźć zastosowanie w innych poza Policją podmiotach, mających uprawnienia do zdobywania i gromadzenia informacji. Właściwie oceniona, a następnie bezpiecznie zmagazynowana informacja staje się punktem wyjścia dla ich analizy. Rolą analizy kryminalnej jest sprawne wykorzystanie zgromadzonych w zasobach bazodanowych informacji, poprzez wyszukanie relacji i powiązania (w danej sprawie) w logiczną całość dającą podstawy pod dalsze wnioskowanie.

Obok przedstawiono tabelę ukazującą ocenę wiarygodności informacji.

Techniki i narzędzia wykorzystywane w procesie analizy kryminalnej

Techniki stosowane w analizie kryminalnej

Zaprezentowane w niniejszym podrozdziale techniki stosowane w analizie kryminalnej zostały ujednolicone w celu uproszczenia ich zastosowania i interpretacji. Aby ocenić ich uniwersalizm i tym samym możliwość wykorzystania w wielu podmiotach i obszarach działań należy zapoznać się z charakterystyką poszczególnych technik i zasad ich wizualizacji.

Wizualizacja informacji

Techniki analityczne sprowadzają się do wizualizacji informacji zawartych w posiadanym materiale, które zostały wyselekcjonowane przez analityka spośród „chaosu informacyjnego", a następnie przestawione wg przyjętych dla danej techniki reguł. Większość informacji i danych zawartych w aktach sprawy (także na innych nośnikach) ma charakter nieuporządkowany. Zarówno systematyzacja materiału jak i dobór informacji do jego zobrazowania jest wynikiem autorskiej koncepcji analityka. Tworzenie diagramów odzwierciedlających informacje nie jest odkrywcze, stosowane jest praktycznie w każdej dziedzinie nauki. Diagramy dają podstawę szybkiej percepcji złożonych zagadnień i w efekcie szybszego i bardziej merytorycznego wnioskowania.

Wizualizacja informacji według wybranej techniki analitycznej pełni w analizie kryminalnej dwojaką rolę. Po pierwsze – jest elementem warsztatu pracy analityka, który budując diagram zwany „roboczym" przetwarza na nim dużą liczbę informacji i jest wówczas w stanie łatwiej zrozumieć, jak również ocenić i wyszukać zależności. W praktyce są to diagramy mocno skomplikowane, jednakże z uwagi na to, iż analityk sam tworzy ten diagram poświęcając mu wiele uwagi, jest w stanie „opanować" zakres informacji o obiektach analitycznych i połączeniach między nimi. Wizualizacja jest także produktem służącym analitykowi do nawiązania kontaktu z odbiorcą analizy. Stanowi pomost pomiędzy informacjami tekstowymi, a ich graficznym

		KOD OCENY INFORMACJI Stosunek źródła do informacji			
KOD OCENY ŹRÓDŁA Ocena wiarygodności źródła		**Informacja jest prawdziwa bez jakichkolwiek zastrzeżeń**	**Informacja jest znana osobiście źródłu informacji**	**Informacja nie jest znana źródłu osobiście, ale jest potwierdzona przez inne informacje już znane**	**Informacja nie jest znana osobiście źródłu i nie może zostać potwierdzona w żaden inny sposób**
		1	**2**	**3**	**4**
Nie ma wątpliwości, co do autentyczności, wiarygodności i kompetencji źródła informacji lub informacja pochodzi od źródła, które udowodniło swoją wiarygodność we wszystkich możliwych przypadkach w przeszłości	**A**	A1 Funkcjonariusz policji, sądu, prokuratury, metody pracy policji, procesowo udowodnione wyniki	A2 Funkcjonariusz policji, sądu, prokuratury, metody pracy policji, procesowo udowodnione wyniki	A3 Funkcjonariusz policji, sądu, prokuratury, metody pracy policji, procesowo udowodnione wyniki	A4 Funkcjonariusz policji, sądu, prokuratury, metody pracy policji, procesowo udowodnione wyniki
Informacja pochodzi ze źródła, które w większości przypadków było wiarygodne	**B**	B1 Inni funkcjonariusze administracji państwowej Bazy danych m.in. ZSIP, KSIP, OPIS, TBD WEP, Temida, wypisy z ksiąg wieczystych, itp., OZI o długoletnim stażu współpracy, który zawsze się sprawdzał	B2 Inni funkcjonariusze administracji państwowej Bazy danych m.in. ZSIP, KSIP, OPIS, TBD WEP, Temida, wypisy z ksiąg wieczystych, itp., OZI o długoletnim stażu współpracy, który zawsze się sprawdzał	B3 Inni funkcjonariusze administracji państwowej Bazy danych m.in. ZSIP, KSIP, OPIS, TBD WEP, Temida, wypisy z ksiąg wieczystych, itp., OZI o długoletnim stażu współpracy, który zawsze się sprawdzał	B4 Inni funkcjonariusze administracji państwowej Bazy danych m.in. ZSIP, KSIP, OPIS, TBD WEP, Temida, wypisy z ksiąg wieczystych, itp., OZI o długoletnim stażu współpracy, który zawsze się sprawdzał
Informacja pochodzi ze źródła, które w większości przypadków nie było wiarygodne	**C**	C1 Większość informacji pochodzących od OZI, wymagających dodatkowej weryfikacji	C2 Większość informacji pochodzących od OZI, wymagających dodatkowej weryfikacji	C3 Większość informacji pochodzących od OZI, wymagających dodatkowej weryfikacji	C4 Większość informacji pochodzących od OZI, wymagających dodatkowej weryfikacji
Informacja pochodzi z nowego, niesprawdzonego źródła, którego autentyczność, kompetencje i wiarygodność nie są znane lub informacja pochodzi z nowego, niesprawdzonego źródła, którego autentyczność, wiarygodność oraz kompetencje nie mogą być potwierdzone	**X**	X1 Świeżo pozyskane źródła (OZI), których wiarygodność do tej pory nie jest znana, świadek, źródeł nieustalonych, wysoce niepewnych, przekazujących informacje jednorazowo, lub które przekazując informacje wyraźnie celowo „żonglują" posiadaną wiedzą – wszystkie media – wszelka prasa, radio, TV, czy Internet	X2 Świeżo pozyskane źródła (OZI), których wiarygodność do tej pory nie jest znana, świadek, źródeł nieustalonych, wysoce niepewnych, przekazujących informacje jednorazowo, lub które przekazując informacje wyraźnie celowo „żonglują" posiadaną wiedzą – wszystkie media – wszelka prasa, radio, TV, czy Internet	X3 Świeżo pozyskane źródła (OZI), których wiarygodność do tej pory nie jest znana, świadek, źródeł nieustalonych, wysoce niepewnych, przekazujących informacje jednorazowo, lub które przekazując informacje wyraźnie celowo „żonglują" posiadaną wiedzą – wszystkie media – wszelka prasa, radio, TV, czy Internet	X4 Świeżo pozyskane źródła (OZI), których wiarygodność do tej pory nie jest znana, świadek, źródeł nieustalonych, wysoce niepewnych, przekazujących informacje jednorazowo, lub które przekazując informacje wyraźnie celowo „żonglują" posiadaną wiedzą – wszystkie media – wszelka prasa, radio, TV, czy Internet

Tab. 2. Ocena wiarygodności informacji (źródło: opracowanie własne na podstawie materiałów informacyjnych BWK KGP)

odwzorowaniem. Pracując na diagramie roboczym, analityk następnie tworzy diagram końcowy wybierając odpowiedni układ (np. hierarchiczny, odśrodkowy), usuwa zbędne przecięcia linii, dokonuje uproszczeń (rezygnacja z elementów mało istotnych, które można zastąpić krótkim komentarzem, legendą). Efekt analizy zostanie osiągnięty, jeśli diagram (diagramy) końcowy będzie przejrzystym przewodnikiem po raporcie (sprawozdaniu) analityka, gdzie z jednej strony sam w sobie stanowi źródło pewnych informacji (czasem nawet inspiracji), a z drugiej ułatwia odczytywanie kolejnych treści raportu odwołujących się do diagramu.

Przetworzenie informacji tekstowej na „obraz" nie jest, wbrew pozorom, prostym zabiegiem, odbywa się w sposób metodyczny z zachowaniem pewnych ogólnych zasad, związanych z celem, przyjętym układem, czytelnością i aktualnością diagramu.

Cel diagramu

Każdy diagram czemuś służy, tak więc obranie celu diagramu dokonuje się równolegle z doborem techniki analitycznej. Cel diagramu zostaje osiągnięty sposobem projekcji informacji składających się na końcowy „obraz". Fizycznie zostaje uwidoczniony zazwyczaj w tytule diagramu bądź w opisie, np. diagram powiązań kapitałowych firmy „X". Tytuł ten zawiera informację o wybranej technice analitycznej (diagram powiązań) oraz czemu ona służyła (przedstawieniu powiązań kapitałowych wybranego podmiotu).

Układ diagramu

Zaprojektowanie diagramu, jego wyglądu, wiąże się z doborem odpowiedniego układu – graficznego rozplanowania elementów. W dużej mierze dobór techniki analitycznej determinuje sposób zagospodarowania przestrzennego diagramu, jednak od analityka zależy w jakiej perspektywie to nastąpi. Jeżeli ma być pokazana hierarchia danej organizacji, wówczas dobrze jest zaprezentować układ strukturalny od obiektów zwierzchnich do podległych (od góry do dołu). Można tu także wyróżnić poszczególne poziomy obiektów stanowiących równorzędny szczebel organizacji. Układ odśrodkowy przedstawia najistotniejszy obiekt (obiekty) w środku, z odchodzącymi od niego rozgałęzieniami (powiązaniami z innymi obiektami), nazywany również „pawim ogonem" (komenda polecenia w menu oprogramowania analitycznego). Z kolei diagramy chronologiczne można przedstawić w układzie proporcjonalnym upływu czasu pomiędzy poszczególnymi zdarzeniami (ale wówczas można narazić się na wydłużenie diagramu „pustymi" okresami, bez żadnych składowych zdarzeń) lub np. w zgrupowanym układzie, oznaczającym brak proporcji podziałki czasu względem poszczególnych informacji o zdarzeniach tak, aby na jak najmniejszej powierzchni zmieściły się poszczególne ramki zdarzeń z zachowaniem ich kolejności (chronologii).

Czytelność diagramu

Łatwość interpretacji diagramu zależy od jego przejrzystości. Im bardziej ograniczy się liczbę obiektów naniesionych na diagram, tym bardziej będzie on czytelny. Należy unikać: krzyżowania się linii łączących obiekty lub ich załamywania (w miarę możliwości), stykania się obiektów, nachodzenia na siebie opisów, stosowania nadmiaru kolorów bądź zbędnego

„ozdabiania" diagramu. Czytelność diagramu łączy się z jego percepcją przez osoby, dla których został stworzony, a – jak już wspomniano – jest on swoistym „przewodnikiem" po informacjach, więc jego czytelność wpłynie na całościowy odbiór analizy. Najczęściej analitycy pracują na tzw. „diagramie roboczym" (obejmuje większość informacji odwzorowanych na grafie), który następnie można przekształcić na postać bardziej czytelną, a tę prezentuje się odbiorcom analizy kryminalnej. Pozostawia się na diagramie najistotniejsze obiekty analityczne i powiązania wraz z dołączonym opisem (każdy diagram musi być opatrzony komentarzem, odniesieniem do materiału).

Aktualność

Każdy diagram powstaje w oparciu o konkretne informacje. Informacje te, zawarte w ponumerowanych kartach akt (innych nośnikach), dotyczą stanu na dany dzień. Diagram zachowuje aktualność na daną chwilę, tj. czas, w którym analityk pracuje na określonej liczbie informacji, uzyskanej w określonym momencie. Należy oznaczyć każdy diagram datą wykonania (czasami również godziną), dzięki czemu wiadomo później dlaczego nie zawiera on np. informacji uzyskanych już po jego sporządzeniu i jednocześnie pozwala na zachowanie chronologii. Powyższe wskazówki mają charakter uniwersalny, dotyczą wszystkich sposobów wizualizacji informacji, odnosząc się przede wszystkim do wskazanych na wstępie ról, jakie zasadniczo powinna ona pełnić.

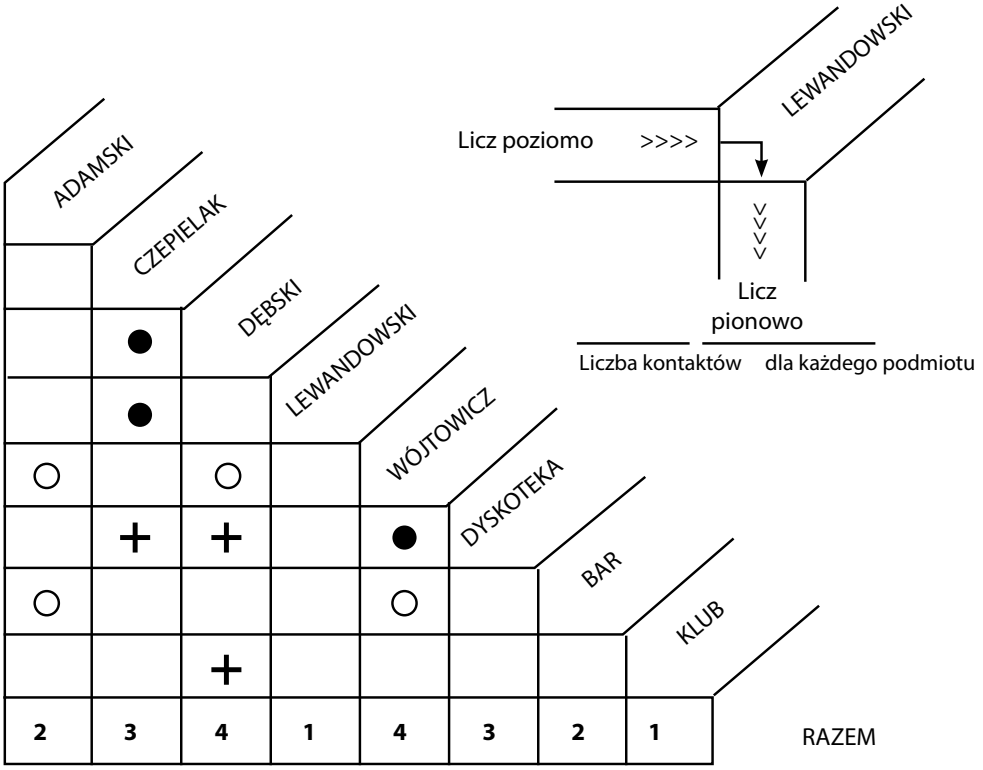
Zaprezentowane dalej techniki analityczne znajdują odzwierciedlenie w praktyce, zwłaszcza w odniesieniu do kryminalnej analizy operacyjnej. Wynika to z różnic w zakresie omawianych wcześniej rodzajów i form analizy kryminalnej (analiza strategiczna może opierać się na odmiennej metodologii często zapożyczonej, np. CRISP-DM125).

Matryca – element pracy z diagramem

Przed przystąpieniem do odwzorowania informacji na graf (głównie diagram powiązań) można posiłkować się matrycą (schemat 2.). Zadaniem matrycy jest uporządkowanie i wylistowanie obiektów oraz zaznaczenie zachodzących pomiędzy nimi relacji. Ma charakter pomocniczy w tworzeniu diagramu, pozwala na późniejszą jego kontrolę pod kątem zgodności danych zawartych w matrycy i na wykresie.

Nanoszenie powiązań pomiędzy obiektami w matrycy odbywa się także przy pomocy odpowiedniego kodowania, które koresponduje z systemem oceny źródła i informacji „4x4" Kodowanie matrycy ma na celu właściwe zaznaczenie faktu wystąpienia relacji wiążącej dane obiekty analityczne oraz jej charakteru (np. informacje potwierdzone – niepotwierdzone).

Rzetelnie wypełniona matryca daje gwarancje zachowania wszystkich interesujących powiązań występujących w materiale (uwzględniających osoby „funkcyjne" oznaczane symbolem „+"), pozwala na ustalenie liczby obiektów z największą liczbą powiązań, stanowi punkt wyjściowy dla tworzenia diagramu powiązań, zwłaszcza diagramu roboczego. Matryca może być także wykorzystana do zestawienia statystycznego kontaktów osoby z inną osobą lub obiektem, wskazania, które osoby i w jakim czasie uczestniczyły w danym zdarzeniu, miejscu etc.



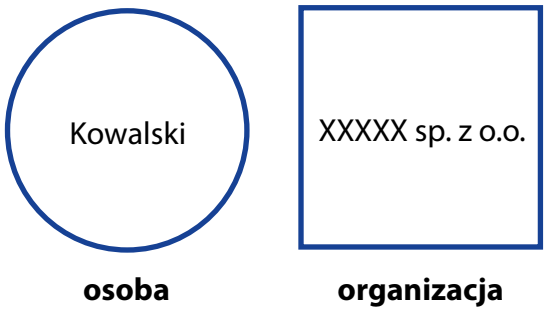
Rys. 2. Wypełniona matryca powiązań (źródło: W. Iganczak, *Wybrane zagadnienia analizy kryminalnej*, Szczytno 2005)

Diagramy powiązań

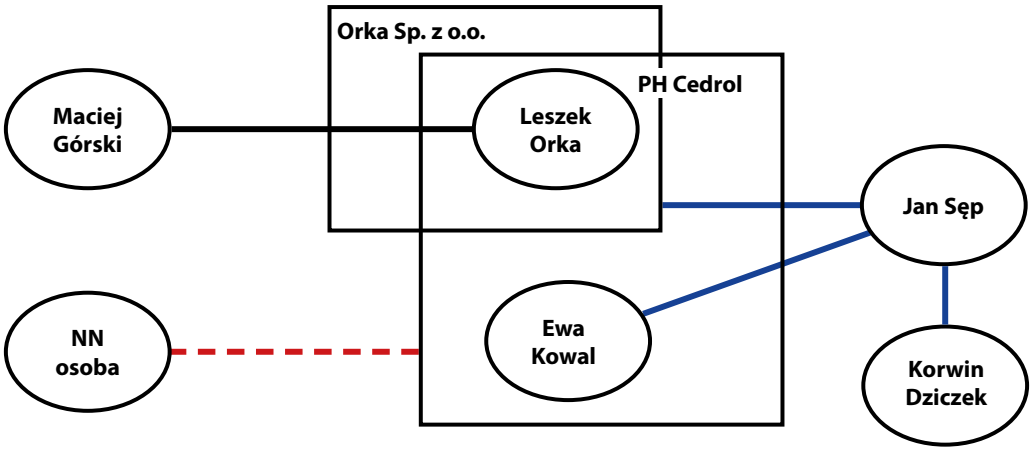
Diagram powiązań jest graficzną projekcją relacji zachodzących pomiędzy osobami, organizacjami czy przedmiotami występującymi w prowadzonej sprawie. Wzajemne powiązania dotyczą dowolnych konfiguracji personalnych oraz zaistniałych pomiędzy osobami, a organizacjami lub przedmiotami, a także pozostałych związków bez udziału osób. Jest on techniką analityczną, która znaleźć może zastosowanie w każdej sprawie o ile występuje taka konieczność. Oczywiste, proste układy relacyjne nie wymagają wizualizacji (np. powiązania tylko kilku obiektów), ale każdorazowo ma to indywidualny wymiar oceny.

W analizie kryminalnej przyjęte zostały jednolite sposoby wizualizacji informacji poprzez zastosowanie prostej symboliki. Zanim masowo zaczęto używać komputerów i opracowano dedykowane aplikacje komputerowe, wykorzystano dwie figury geometryczne do reprezentowania określonych obiektów analitycznych. Okręgiem oznaczano osoby, zaś prostokątem organizacje (rysunek 3.), rozumiane szerzej, jako wszelkie inne aniżeli osoby obiekty analityczne (organizacje przestępcze, adresy, miejsca, podmioty gospodarcze itp.).

Analityk kryminalny może przedstawiać informacje potwierdzone i niepotwierdzone odpowiednio linią ciągłą lub przerywaną, łączącą krawędzie obiektów (jako obiektów powiązanych zgodnie z materiałami sprawy). Osoby, które zarządzają lub mają realny wpływ na funkcjonowanie danej organizacji (np. wynajemca i wynajmowane mieszkanie, firma



Rys. 3. Symbole stosowane w diagramach powiązań (źródło: opracowanie własne)



Rys. 4. Diagram powiązań osób i organizacji (źródło: opracowanie w oparciu o materiały szkoleniowe WSPol)

i właściciel, dyrektor, udziałowiec firmy) przedstawiane są na diagramie owalami znajdującymi się wewnątrz prostokąta (rysunek 4).

Rozwój technologii spowodował wkroczenie rozwiązań komputerowych również w sferę pracy organów ścigania i dostosowanie funkcjonalności powstałych aplikacji analitycznych do zasad wizualizacji stosowanych tradycyjnie. W efekcie możliwości obrazowania wszelkich informacji stały się bardziej zaawansowane graficznie i intuicyjne w przekazie.

Diagramy powiązań mają niebagatelne znaczenie m.in. w prezentowaniu powiązań w zorganizowanych grupach przestępczych, powiązań kapitałowych podmiotów gospodarczych czy obrazowanie sieci społecznościowych. Pozwalają dostrzec obiekty pośredniczące, stanowiące węzły, odgrywające kluczową rolę w przepływie informacji itd. (rysunek 5.). Przy skomplikowanych, rozbudowanych sieciach analitycy zaprezentować mogą ogólny obraz powiązań, ujmując na nim główne linie odzwierciedlające relacje pomiędzy najistotniejszymi obiektami, a następnie, stosując „rozwinięcie" obrazu wyjściowego na kilka, uściślają wybrane fragmenty na oddzielnych diagramach (od ogółu do szczegółu). Uzyskuje się dzięki

temu wstępny obraz całości najistotniejszych powiązań, a następnie uwaga kierowana jest na drobniejsze rozbudowane odnogi sieci relacyjnej. Ten sposób prezentowania powiązań można także odwrócić, stosując zasadę „od szczegółu do ogółu". Jak zawsze zależne jest to od koncepcji analityka i tego, do kogo adresuje swoją wypowiedź (ustną bądź pisemną).

Diagramy przepływu towaru i usług

Diagramy przepływów mają za zadanie ukazanie faktycznego przemieszczania się towaru (materialnego lub niematerialnego) od danego obiektu do drugiego (np. od osoby do osoby czy z miejsca na miejsce). Nie różnią się znacznie od diagramów powiązań (obiekty analityczne przedstawiane są także w postaci okręgów i prostokątów), w miejsce połączeń pojawiają się strzałki, które wskazują kierunek przepływu danego towaru rysunek 6.).

Pozwalają, np. wskazać najsłabsze ogniwo w obiegu towaru, czy dokonać próby bilansu w przypadku posiadania chociaż szczątkowych czy orientacyjnych wiadomości na temat przepływających ilości (jednostki wag i miar).

Diagramy przepływów towarów i usług są techniką niezwykle pomocną w przypadku konieczności analizy danych uzyskanych z różnych źródeł (często liczących tysiące rekordów np. bilingi telefoniczne, transakcje bankowe), w których mamy do czynienia z kierunkiem transferu określonego „dobra". Następnie konieczne jest ich zaprezentowanie w postaci zrozumiałej dla zleceniodawcy, zgodnie z jego oczekiwaniami. Oprócz samej wizualizacji obiektów analitycznych, wykorzystywane są narzędzia analityczne oprogramowania (np. wyliczenia matematyczne, odniesienie do dat, dni tygodnia etc.

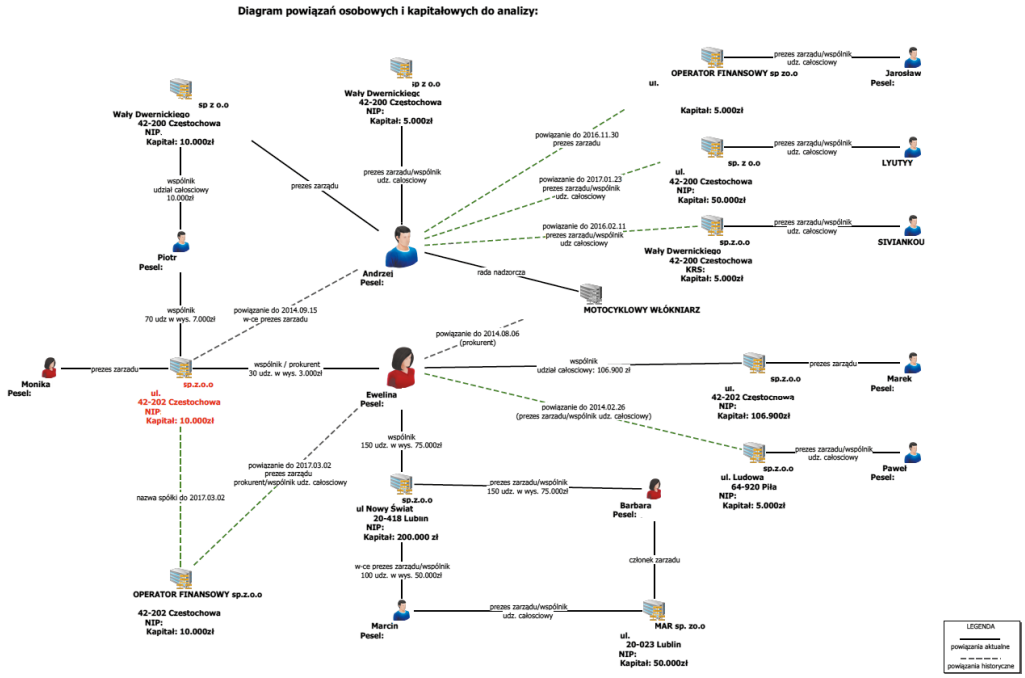
Diagramy chronologii zdarzeń

Diagramy chronologiczne, obrazujące układy zdarzeń, ich kolejności i wzajemnego oddziaływania pozwalają spojrzeć na zagadnienie przez pryzmat czasu. Aby utworzyć diagramy chronologiczne na podstawie danej sprawy, zagadnienia, fragmentu rzeczywistości należy odseparować zbiór informacji składających się na ciąg poszczególnych drobnych zdarzeń, te natomiast przełożą się na całość wydarzenia (zjawiska). Przedstawiane są w postaci diagramów wydarzeń i analizy chronologii zdarzeń.

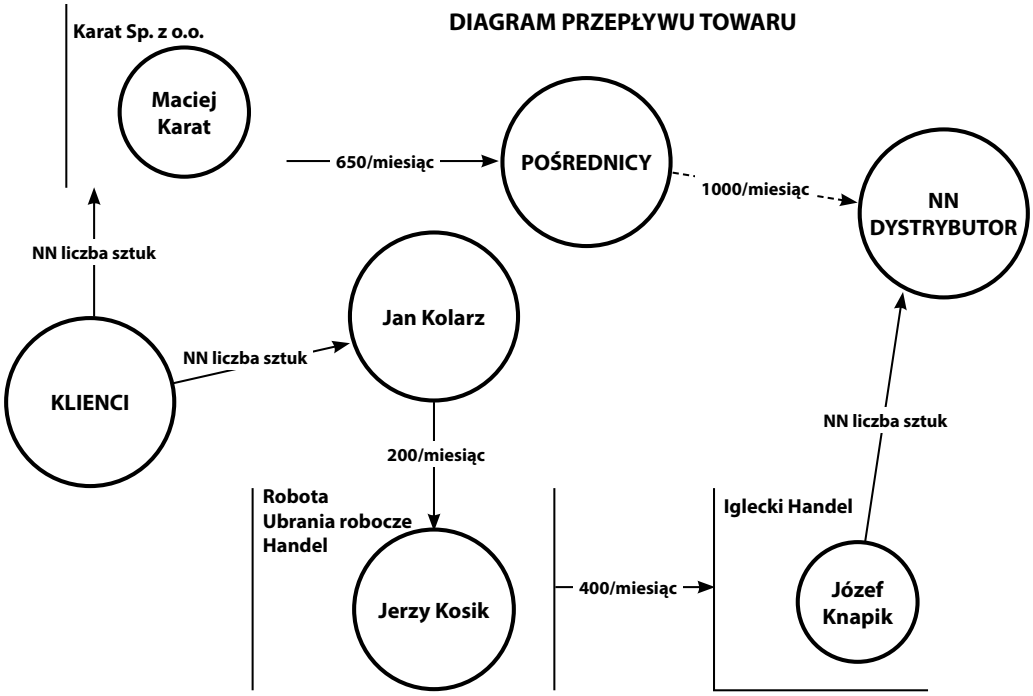
Diagramy wydarzeń przedstawia się w postaci ułożonych chronologicznie opisów poszczególnych zdarzeń (z obrysem wokół tekstu), połączonych strzałką (od lewej do prawej strony). W prosty i stosunkowo szybki sposób pozwalają przedstawić najistotniejsze zagadnienia uwzględniające upływ czasu. Czas opisywany jest w ramkach zdarzeń lub/oraz na osi czasu umieszczonej powyżej diagramu (rysunek 8.).

Diagramy określane jako analiza chronologii zdarzeń są bardziej rozbudowane graficznie. Oprócz ramek zdarzeń analogicznych jak w diagramach wydarzeń, wykorzystuje się tzw. linie tematu, którymi oznaczane są najczęściej osoby, firmy, telefony, rachunki bankowe, działania (również przestępstwa) i inne (rysunek 9.).

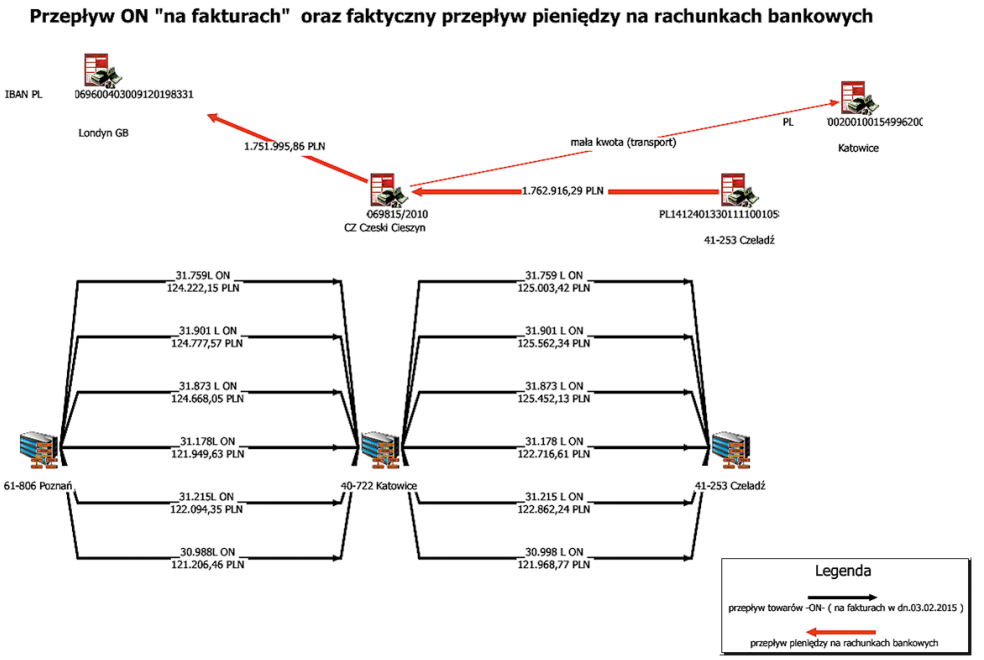
Na linii tematu biegnącej wzdłuż osi czasu nanosi się ramki zdarzeń, które są z nią związane merytorycznie. Niektóre zdarzenia spajają dwie lub więcej linie tematów. Wykonywane połączenia telefoniczne lub przelewy bankowe obrazowane są w postaci strzałek (pionowo) łączących konkretne linie tematu z ukazaniem kierunku nawiązywanego połączenia



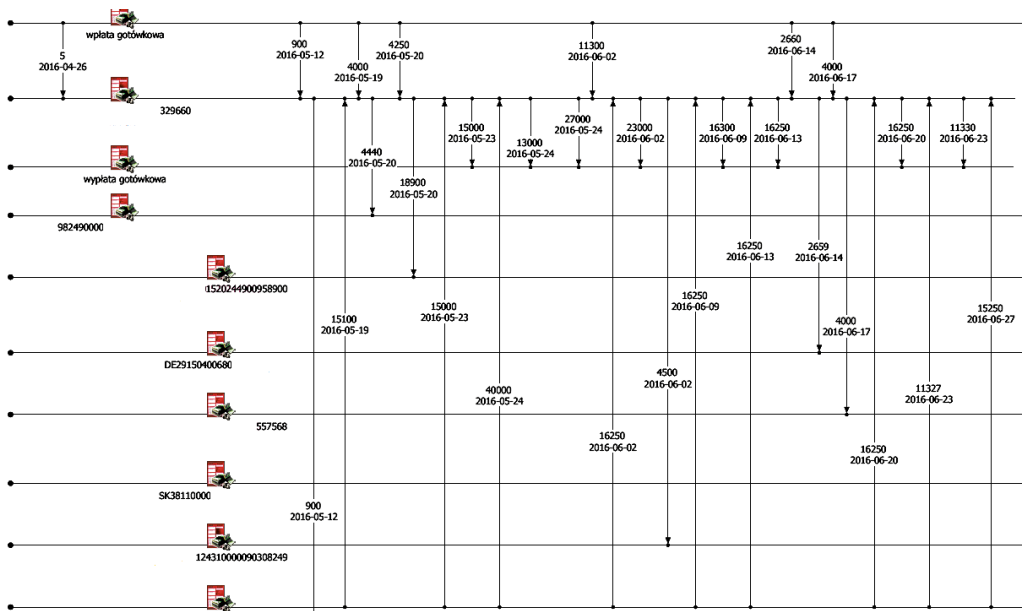
Rys. 5. Diagram powiązań wykonany przy użyciu aplikacji i2 Analyst's Notebook (źródło: opracowanie własne)



Rys. 6. Diagram przepływu towaru z zastosowaniem „tradycyjnej" symboliki (źródło: W. Iganczak, *Wybrane zagadnienia analizy kryminalnej*, Szczytno 2005)



Rys. 7. Diagram przepływu wykonany w aplikacji Analyst's Notebook (źródło: opracowanie własne – dla potrzeb przedmiotowej pracy usunięto dane identyfikacyjne podmiotów i rachunków)



Rys. 8. Chronologiczny diagram przepływów finansowych (źródło: opracowanie własne – dla potrzeb przedmiotowej pracy dane identyfikacyjne zostały usunięte)

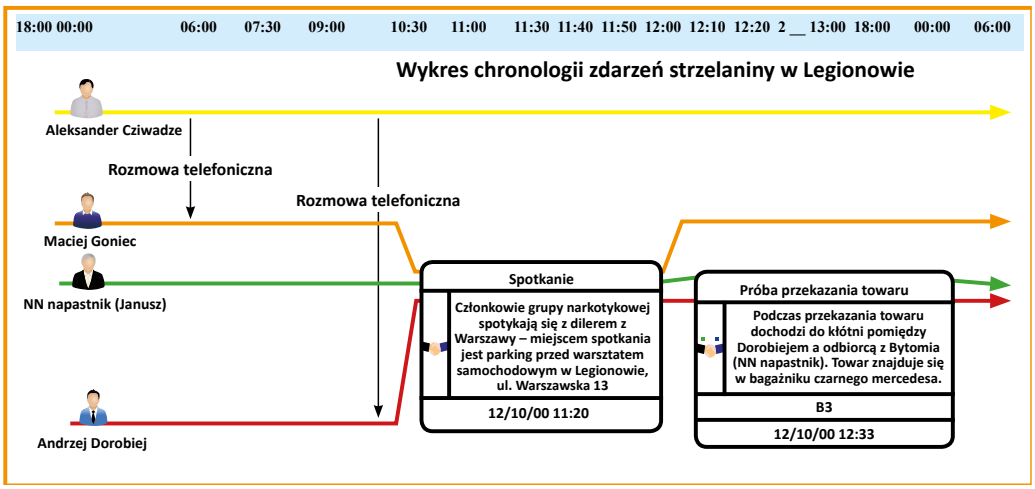
telefonicznego lub operacji finansowych. Linie tematów zmuszają do śledzenia zdarzeń przypisanych do nich indywidualnie bądź zbiegających się z innymi liniami, jeśli zdarzenie dotyczy większej liczby tematów. Pozwalają na wieloaspektowe analizowanie zależności w czasie danych i informacji, związków przyczynowo – skutkowych, wskazywania luk w materiałach lub tzw. „kolizji zdarzeń", tj. informacji wzajemnie się wykluczających. Diagramy te dają doskonałe pole do stawiania hipotez i ich weryfikacji.

Przykładowo w sprawie „X" zeznaje czterech świadków relacjonując przebieg wydarzeń z konkretnych dwóch dni. Każdy z nich przedstawia wersję taką, jaką pamięta lub chce, aby na taką wyglądała. Dysponujemy więc czterema liniami, na których umieszczane są elementy składające się na ciąg całego wydarzenia, przy czym opisy bądź umiejscowienie w czasie tych zdarzeń różnią się. Opracowany w ten sposób diagram pozwoli wychwycić wszelkie różnice, nieścisłości poddać analizie, a ponadto przygotować się do dalszych czynności (np. do opracowania planu konfrontacji świadków) lub dotrzeć do innych źródeł informacji, które umożliwią weryfikację dotychczasowych informacji (np. zapisy monitoringu, inni świadkowie).

Analiza chronologii zdarzeń to technika stosowana zwłaszcza przy wykorzystaniu oprogramowania analitycznego, gdzie diagramy mogą być również generowane automatycznie. Za ich pomocą można zestawiać różnego rodzaju informacje (np. dane z faktur z danymi transportowymi, dane z systemów bankowych z dokumentacją firmy).

Diagramy działalności

Zadaniem diagramów działalności jest ukazanie mechanizmu działania przestępczego w postaci uniwersalnego szablonu, który można „przyłożyć" do każdego typu danego przestępstwa. Odpowiadając na pytanie: jak coś zostało zrobione?, diagram ten ma mieć przełożenie na przyszłość i udzielić odpowiedzi na zmodyfikowane pytanie: jak coś może być zrobione?



Rys. 9. Diagram chronologii zdarzeń przedstawiający linie tematyczne i ramki zdarzeń (źródło: M. Hausman, *Wykorzystanie analizy kryminalnej w działaniach podmiotów realizujących zadania na rzecz bezpieczeństwa Rzeczypospolitej Polskiej*, Wyższa Szkoła Policji w Szczytnie, Szczytno 2014)

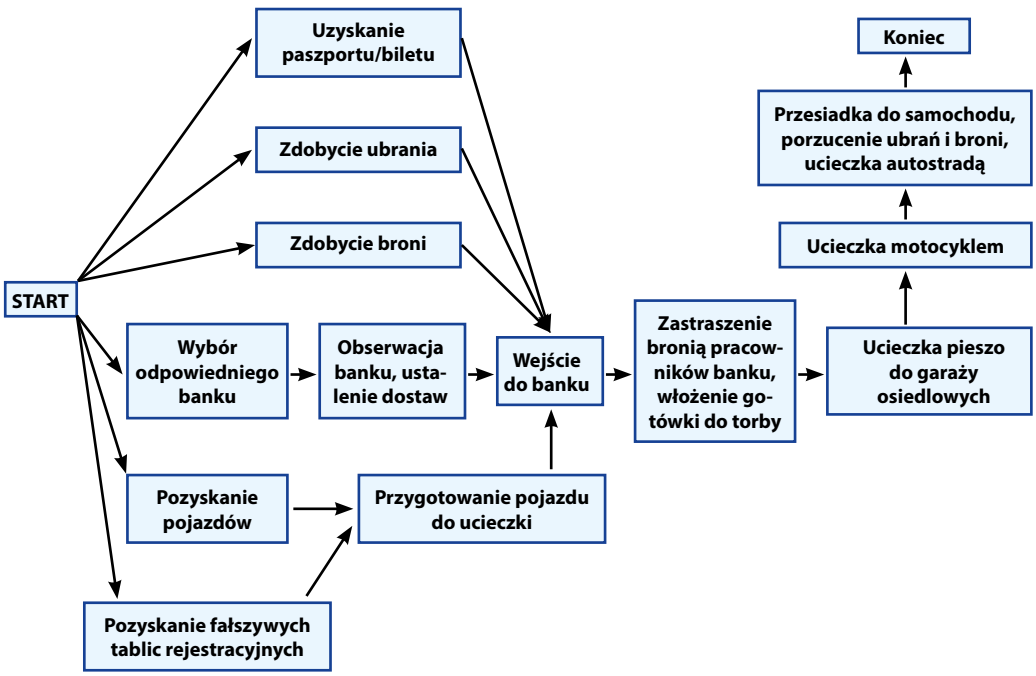
Sposób ich tworzenia jest analogiczny do diagramów wydarzeń. Zasadnicza różnica polega na tym, iż diagramy wydarzeń dotyczą konkretnego przypadku, jego indywidualnego przebiegu z uwzględnieniem czasu każdego drobnego zdarzenia, składającego się na analizowane wydarzenie, natomiast w diagramach działalności ukazuje się zestaw działań do wykonania bez osadzania ich w konkretnym czasie.

Przestudiowanie działań podejmowanych w ramach danego przestępstwa prowadzi do ułożenia ich na liniach czynności zależnych i niezależnych od siebie. Jedne z czynności warunkują następne, część z nich może być wykonywana bez wpływu na inne (np. założenie strony internetowej firmy nie wymaga rozliczenia podatku VAT, mogą one zachodzić niezależnie od siebie). W efekcie tworzy się modele działań, które mogą być przydatne nie tylko w fenomenologicznym ujęciu aktywności grup przestępczych, ale również np. w odniesieniu do działalności antyterrorystycznej, czy też podejmowanej dla zapewnienia bezpieczeństwa systemów informatycznych (również w ramach wszelkich innych zagadnień, w których uwidacznia się powtarzalny zestaw czynności).

Analiza porównawcza

Jak już wspomniano przy omawianiu form analizy operacyjnej, analiza porównawcza przestępstw zmierza do ustalenia czy dane przestępstwa (zachowania) mogły zostać dokonane przez tego samego sprawcę lub grupę.

WYKRES DZIAŁAŃ WSKAZUJĄCY NA METODY ORAZ UCIECZKĘ W PRZYPADKU SERII NAPADÓW NA BANKI



Rys. 10. Diagram działalności (źródło: opracowanie własne w oparciu o materiał szkoleniowy)

Czynności analityczne polegają na określeniu kryteriów, zgodnie z którymi porównuje się poszczególne sprawy. Sam dobór kryteriów jest niezwykle istotny, gdyż nie wszystkie cechy występują w każdej ze spraw. Unikać należy kryteriów niejasnych, budzących wątpliwości interpretacyjne, natomiast muszą one we wspólnym zestawieniu ukazywać zbieżności bądź rozbieżności posiadanych cech, by na tej podstawie ocenić później stopień prawdopodobieństwa seryjności lub całkowicie go wykluczyć. Technicznie analiza taka prowadzona jest z wykorzystaniem tabeli, w której zestawiane są z jednej strony określone kryteria porównywania, a z drugiej wyselekcjonowane do porównania sprawy (tabela 3.).

Analiza porównawcza dokonywana z użyciem techniki tabelarycznej, finalnie sprowadzać się będzie do wychwytywania najistotniejszych cech zbieżnych w porównywanych przypadkach, jak również cech różnicujących. Dokonywać się będzie zatem analiza ilościowa (cech zbieżnych), ale przede wszystkim jakościowa. Obie one ostatecznie wpłyną na sposób określenia stopnia prawdopodobieństwa seryjności przez analityka kryminalnego. Oczywiście analiza taka nie sprowadza się wyłącznie do zestawienia w tabeli cech charakterystycznych przestępstw. Zarówno przed, jak i po niej dokonywane jest wnikliwe badanie akt i zebranego w sprawie materiału.

Każda z wymienionych i opisanych technik analitycznych znajduje swoje zastosowanie głównie w kryminalnej analizie operacyjnej. Ze względu na uniwersalizm, sprowadzający się do badania informacji od różnego rodzaju źródeł, mogą one być wykorzystane w pracy wielu podmiotów, które podejmują decyzje bieżące bądź strategiczne na podstawie zasobów informacyjnych.

Każda z wymienionych i opisanych technik analitycznych znajduje swoje zastosowanie głównie w kryminalnej analizie operacyjnej. Ze względu na uniwersalizm zastosowania w pracy z różnego rodzajami źródeł informacji, mogą one zostać wykorzystane w pracy wielu podmiotów, które podejmują decyzje bieżące bądź strategiczne na podstawie zasobów informacyjnych.

Narzędzia stosowane w analizie kryminalnej

Współcześnie, w dobie pełnej informatyzacji społecznej, pozostawiamy po sobie mnóstwo informacji w postaci elektronicznej korzystając z komputerów PC, tabletów, smartfonów. Wszystkie te informacje, gdy korzystamy ze sklepów internetowych, portali społecznościowych, komunikatorów społecznych, można poddać analizie oraz połączyć ze sobą w jedną spójną i jasną całość. W klasyczny sposób nie uda ich się jednak powiązać, dlatego w tym momencie analityk kryminalny korzysta ze specjalistycznego oprogramowania analitycznego np. Analyst's Notebook, iBase, Link, ArcGIS.

Analyst's Notebook

Analyst's Notebook współpracuje z oprogramowaniem iBase. Oprogramowanie to służy do graficznej prezentacji obiektów i powiązań między nimi w formie wykresów oraz do przetwarzania zebranych informacji. W zależności od rodzaju danych, obiekty przedstawiane są na wykresie jako ikony oraz inne symbole takie jak linie tematów, ramki zdarzeń, prostokąty, kola, bloki tekstu, obiekty OLE. Relacje pomiędzy obiektami przedstawiane są w postaci linii

Włamanie do banku			
Nazwa banku	Bank Ochrony Środowiska w Sxxxxx	Bank Spółdzielczy w D...xxx	Bank Gosp. Region. Jxxxxx..
Adres	Sxxxxxx, ul. Biała 2	D...xxx, ul. XXX-lecia 16	Jxxxxx.., ul. Pola 5
Data	2012-09-25/26	2012-10-08/09	2012-11-15/16
Dzień tygodnia	wtorek / środa	poniedziałek / wtorek	czwartek / piątek
Godz. rozp. włamania	23:40	02:20	00:40
Godz. zakończ. włamania	01:30	03:10	01:50
Godz. ujawnienia	06:20	05:25	02:20
System alarmowy			
Charakterystyka systemu	łączność z centralą: GSM czujki ruchu, zbicia szyb, kamery monitorujące, sygnalizacja dźwiękowa zewnętrzna i wewnętrzna oraz powiadomienie centrali monitorującej	łączność z centralą: TP SA i GSM czujki ruchu, zbicia szyb, otwarcia sejfu i bankomatu, sygnalizacja alarmowa optyczno-dźwiękowa na budynku oraz powiadomienie centrali monitorującej	łączność z centralą: TP SA i GSM czujki ruchu, zbicia szyb, otwarcia sejfu i bankomatu, sygnalizacja alarmowa optyczno-dźwiękowa zewnętrzna i wewnętrzna oraz powiadomienie centrali monitorującej
Montaż	Morski-Systemy Alarmowe	ASsecurity	ASsecurity
Monitoring	Mobilsafe – agencja ochrony	Tarnowski – ochrona obiektów	Mobilsafe – agencja ochrony
Lokalizacja			
Rodzaj miejscowości	miasteczko, siedziba gminy	miasteczko, siedziba gminy	miasto powiatowe
Usytuowanie	przy ulicy bocznej, 200 m od głównej trasy (E-8)	przy głównej drodze (droga gminna)	przy głównej ulicy (droga wojewódzka)
Charakterystyka posesji	posesja ogrodzona, użytkowany tylko przez bank, na terenie posesji budowa nowego budynku oddziału banku budynek wolnostojący, samodzielny, parterowy z poddaszem,	posesja nieogrodzona z parkingiem oświetlonym, wzdłuż ulicy gęste krzaki do wysokości 1,40 m przesłaniające połowę budynku oprócz wejścia, budynek użytkowany wyłącznie przez bank	bank usytuowany w ciągu budynków handlowych, nieogrodzony z bezpośrednim dostępem do wejścia
Rodzaj budynku	budynek wolnostojący, parterowy, użytkowany	budynek wolnostojący, parterowy, użytkowany	Lokal w zabudowie szeregowej, parterowe
Modus operandi			
Pokonanie zabezpieczeń alarmowych	zagłuszenie sygnału GSM odcięcie linii TP SA (w studzience, z punktu widzenie technicznego niepotrzebne), zniszczenie kamer monitorujących i syreny, zabór komputera z zarejestrowanym nagraniem kamer	zagłuszenie sygnału GSM, zniszczenie sygnalizatora dźwiękowego i zewnętrznej kamery monitorującej, zniszczenie centralki alarmu wewnątrz budynku	zagłuszenie sygnału GSM, zniszczenie sygnalizatora optyczno-dźwiękowego i zewnętrznej kamery monitorującej i syren alarmowych, zabór komputera z zarejestrowanym nagraniem kamer
Sposób wejścia	wyrwanie kraty okna z wyważeniem zamka, rozcięcie ściany bankomatu (wew.)	wyrwanie kraty okna z wyważeniem zamka, rozprucie bankomatu wewnątrz budynku	zerwanie i zabranie kłódek z kraty okna w tylnej ścianie, wyważenie okna, rozcięcie bankomatu (wew.), zatarasowanie śmietnikiem drogi dojazdowej od zaplecza banku
Użyte narzędzia	łom, młot, szlifierka kątowa	łom, szlifierka kątowa, wiertarka	łom, młot, szlifierka kątowa

Tab. 3. Tabela porównawcza – włamania do banków (źródło: opracowanie własne, w oparciu o materiały szkoleniowe WSPol)

ciągłych lub przerywanych, bądź strzałek łączących obiekty. W Analyst's Notebook elementy diagramu opisywane są za pomocą etykiety, identyfikatora, opisu i klasyfikacji, czasu, kart informacyjnych, atrybutów i komentarzy. Użytkownik ma możliwość tworzenia i modyfikacji obiektów i atrybutów oraz typów połączeń i tworzenia własnych szablonów diagramu. Użytkownicy oprogramowania maja możliwość bezpośredniego tworzenia diagramów, jak również importowania danych z innych źródeł takich jak: iBase, plik txt czy dane z arkuszy kalkulacyjnych Excell. Szablon importu przygotowywany jest przez użytkownika programu wskazując właściwe ustawienia. Wykorzystując intuicyjne w obsłudze okno dialogowe, analityk określa sposób interpretacji informacji wejściowych (podział na rekordy i pola rekordów) oraz wizualizowania ich w postaci obiektów, połączeń, atrybutów i kart informacyjnych. Analityk określa sposób wypełniania cech obiektów (takich jak identyfikator, etykieta) i łączenie ich wskazując właściwe pola rekordów. Oprogramowanie umożliwia kreowanie różnorakich schematów, uzależnionych od aktualnie wykorzystywanej metody analitycznej. Umożliwia ono przedstawienie struktury powiązań między obiektami lub też uwypuklać chronologię zdarzeń. Software umożliwia przygotowanie wykresów mieszanych, z cechami omówionych wcześniej rodzajów wykresów. Sposób przedstawienia obiektów na diagramie umożliwia automatyczną zmianę na poszczególne układy (układ hierarchiczny, zawierający minimum przecięć, kołowy, pawi ogon, proporcjonalny, uszeregowany, zgrupowany).

Analyst's Notebook posiada liczne funkcje analityczne, tj.:

- wyszukiwanie graficzne pojedynczych elementów oraz elementów połączonych, umożliwiających wyszukiwanie po typie obiektów, kryteriach tekstowych, liczbowych, związanych z datą, po atrybutach, mieszanych,
- wyszukiwania tekstowego obiektów, połączeń, obiektów i połączeń mające możliwość uwzględniania składowych obiektów oraz umożliwiające wyszukiwanie zaawansowane uwzględniające wzorzec zawierający symbole wieloznaczne bądź wyrażenia regularne,
- wyszukiwania pośrednich powiązań pomiędzy obiektami odległymi uwzględniające czas i kierunek połączeń oraz wartości atrybutów obiektów i połączeń,
- wyszukiwania klastrów w grupie połączonych obiektów uwzględniające siłę wiązania oraz wagę połączenia,
- wyszukiwania obiektów podobnych z możliwością definiowania kryteriów porównywanych tekstów,
- umieszczania elementów diagramu w tle, ukrywania wskazanych obiektów,
- tworzenia raportów opierając się na elementach składowych diagramów,
- scalania obiektów.

iBase

Program bazodanowy iBase jest wydajnym i prostym w obsłudze narzędziem wspomagającym proces analizy. Umożliwia ono gromadzenie informacji o obiektach oraz relacjach pomiędzy nimi. Wykorzystywane jest do wspomagania konkretnych dochodzeń, w których jest analityczną bazą integracyjną, ujednolicając standard informacji pochodzących z wielu źródeł. Oprogramowanie iBase posiada wiele cech, lecz najważniejsze z nich to:

- łatwe tworzenie nowych i modyfikacja istniejących wzorów bazy danych, odpowiadających swoistemu charakterowi jednej sprawy (charakterystyczne typy obiektów i powiązań),
- szybkie wprowadzanie informacji dotyczących grup powiązanych obiektów,
- szerokie możliwości importu informacji ze źródeł zewnętrznych,
- obszerny zestaw specjalizowanych funkcji analitycznych,
- pełny związek z Analyst's Notebook,
- łatwość zarządzania,
- skalowalność.

Praca z oprogramowaniem iBase umożliwia tworzenie oraz dostosowywanie układu bazy danych za pomocą czytelnego graficznego interfejsu użytkownika. Układ istniejącej bazy danych można modyfikować podczas prowadzenia czynności dochodzeniowo-śledczych lub operacyjno-rozpoznawczych (np. przez dołączenie nowych typów obiektów, typów połączeń, dołączenie nowych pól do istniejących typów). Jest to szczególnie potrzebne w sytuacji, gdy postępowanie przygotowawcze kieruje się w nowym, nieprzewidzianym wcześniej kierunku,

iBase daje możliwość szybkiego wprowadzania informacji za pomocą tzw. formularzy danych. Formularz danych jest formatką stworzoną specjalnie do tego celu, formułowaną na etapie kreowania projektu bazy. Formatkę można przystosowywać nie tylko do wprowadzania nowych obiektów, ale także do analizowania ich powiązań z obiektami znajdującymi się już w bazie danych.

Oprogramowanie bazodanowe ułatwia import danych pochodzących z różnych typów źródeł, takich jak pliki tekstowe, OLE DB czy pliki XML. Dane wejściowe przetwarzane są na obiekty i połączenia właściwe dla danej struktury bazy, dzięki temu zagwarantowany jest jednolity standard informacji pochodzących z różnych źródeł. Analitycy importują dane za pomocą szablonów importu czyli zbioru u stawie ń definiowanych przez analityka, które określają sposób interpretacji danych wejściowych oraz sposób przetwarzania ich na obiekty i połączenia.

Oprogramowanie iBase zostało opracowane z myślą o analitykach. Zaprojektowano w nim kilkanaście prostych w obsłudze funkcji analitycznych. Za najważniejsze funkcje analityczne uważa się:

- zapytania,
- działania na zbiorach,
- wyszukiwanie rekordów podobnych,
- wzorce podobieństwa z rangą,
- wyszukiwanie tekstu, tworzenie raportów.

Program zapewnia całkowitą integralność iBase z programem Analys's Notebook. W praktyce daje to możliwość wykorzystywania funkcji analitycznych Analys's Notebook w odniesieniu do informacji znajdujących się w iBase. Istotne jest, że ważna część funkcji programu iBase jest dostępna z poziomu Analys's Notebook. Wybór środowiska pracy uzależniony jest wyłącznie od analityka. Kompatybilność z Analys's Notebook rozszerza potencjał analizy poprzez:

- szybką prezentację zależności pomiędzy obiektami ukryty mi w danych na diagramach Analys's Notebook,
- identyfikację połączeń najważniej szych dla danej analizy z wielu różnorodnych połączeń,

- wyszukiwanie, przeglądanie oraz edycja rekordów iBase z poziomu Analys's Notebook,
- tworzenie rekordów obiektów i połączeń iBase z poziomu Analys's Notebook,
- rozwijanie obiektów na wykresach o połączenia i obiekty połączone bez potrzeby powrotu do bazy danych,
- oglądanie rekordów iBase (np. zdarzeń) na wykresach w czasie z uwzględnieniem chronologii.

Administrowanie bazą danych iBase nie stanowi większego problemu. Program zawiera dwa moduły; moduł użytkownika (iBase User) i moduł administratora/projektanta (iBase Designer).

Moduł administratora/projektanta umożliwia opracowywanie struktury baz danych przez definiowanie typów i właściwości obiektów oraz połączeń, ustanawiania zabezpieczeń. Moduł użytkownika predestynuje wykorzystanie baz przez tworzenie lub edycję rekordów oraz analizowanie danych. Zadania projektantów/administratorów to:

- opracowywanie schematów baz danych,
- opracowywanie nowych baz – z zastosowaniem wszystkich niezbędnych typów obiektów i połączeń,
- aktualizowanie projektów istniejących baz przez przygotowanie nowych typów obiektów i połączeń wraz ze zmieniającymi się potrzebami,
- konfigurowanie baz przez przygotowanie list podpowiedzi, schematów etykiet i innych elementów, w zależności od sposobu użytkowania bazy,
- administrowanie, czyli dodawanie użytkowników, ustanawianie zabezpieczeń, usuwanie zbędnych rekordów, tworzenie kopii zapasowych informacji.

Użytkownik natomiast ma za zadanie:

- dodawanie, edycja i usuwanie rekordów,
- przygotowywanie zbiorów i zapytań,
- analizowanie informacji przez zastosowanie różnorodnych funkcji analitycznych,
- przygotowywanie raportów i diagramów,

Link[29]

Środowisko Link stanowi kompleksowe rozwiązanie informatyczne stworzone w celu wspierania pracy analityków kryminalnych. Podstawowa wersja systemu udostępnia zestaw narzędzi do integracji, wstępnego przetwarzania oraz wizualizacji informacji pochodzących z różnych źródeł, a w szczególności bilingów telefonicznych. Link stanowi także platformę integracji różnych metod (pół)automatycznej analizy informacji, które mogą zostać dołączone do systemu w postaci niezależnie wytworzonych komponentów

Link pozwala na wczytywanie danych bilingowych oraz innych danych o charakterze grafowym (w postaci tabeli) wprost z oryginalnych plików. Możliwość szybkiego importu wykorzystująca zdefiniowane szablony pozwala analitykowi na wczytywanie zewnętrznych danych do programu w ciągu kilku sekund. Wraz z systemem dostarczone są szablony importujące bilingi telefoniczne pochodzące od wszystkich polskich operatorów sieci telefonii

[29] Program opracowany przez Zespół Inteligentnych Systemów Informacyjnych, Katedry Informatyki Akademii Górniczo-Hutniczej w Krakowie, https://fslab.agh.edu.pl/ (10.05.2017).

komórkowych. Zaawansowani analitycy mogą również tworzyć nowe szablony i przesyłać je pozostałymi analitykom, co pozwala na szybkie dostosowanie aplikacji do zmieniających się formatów danych.

Zestaw narzędzi analitycznych w budowany w środowisko Link umożliwia analitykowi wykonywanie skomplikowanych operacji za pomocą kilku kliknięć myszką. Narzędzia takie jak: inteligentne łączenie wielu bilingów wykrywające te same numery i połączenia telefoniczne, unifikacja numerów telefonów1, statystyki połączeń telefonicznych czy filtrowanie informacji, pozwalają na przeprowadzenie skutecznych analiz na masowych danych bez konieczności tworzenia bardzo dużych i nieczytelnych wykresów.

Jednym z głównych elementów środowiska Link jest wizualizacja danych bilingowych i grafowych na wykresach ukazujących strukturę zależności informacji. Zestaw rozmaitych rozkładów elementów pozwala analitykowi na wychwycenie istotnych danych w różnych przypadkach, z który mi spotyka się w codziennej pracy. Dodatkowo, różne widoki tych samych danych na wykresie (np., struktura połączeń telefonicznych oraz relacje pomiędzy numerami telefonów i numerami IMEl), pozwalają użytkownikowi na prowadzenie różnych analiz bez konieczności ponownego importu tego samego bilingu. Wraz z edytorem, Link dostarcza zestaw narzędzi do przygotowania raportów1 końcowych będących materiałem dowodowym w prowadzonych sprawach. Paleta elementów, zaawansowana edycja właściwości wizualnych, notatki to przykłady narzędzi, dzięki którym analityk może swobodnie opracować wykres, tak aby w czytelny sposób przedstawiał wyniki analiz. Środowisko Link stanowi kompleksowe rozwiązanie informatyczne stworzone w celu wspierania pracy analityków kryminalnych. Podstawowa wersja systemu udostępnia zestaw narzędzi do integracji, wstępnego przetwarzania oraz wizualizacji informacji pochodzących z różnych źródeł, a w szczególności bilingów telefonicznych. Link stanowi także platformę integracji różnych metod (pół)automatycznej analizy informacji, które mogą zostać dołączone do systemu w postaci niezależnie wytworzonych komponentów.

Etapy czynności analitycznych

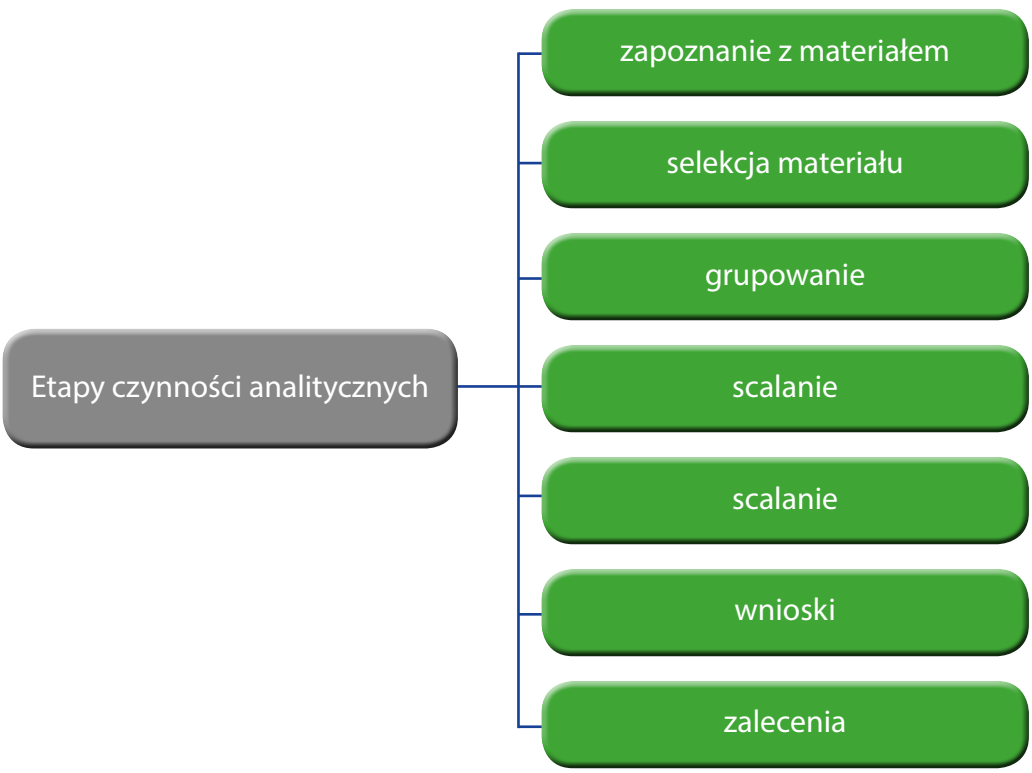
Analiza kryminalna wiąże się z wykonywaniem następujących po sobie czynności. W klasycznym ujęciu cyklu analitycznego stanowi krąg działań, które mając powtarzalny charakter zmierzają do uzyskania finalnych wniosków i planu dalszego postępowania.

Przebieg analizy określają dwa etapy: na pierwszy składają się pozyskiwanie informacji, ich selekcja i ocena, a w drugim etapie przedstawiane są hipotezy śledcze w sprawie. Analityk może te hipotezy zilustrować na wiele sposobów, przedstawiających różne scenariusze (odnoszące się do tego, co było bądź dopiero się wydarzy), które mają uzasadnić te hipotezy.

Jako element procesu zarządzania informacją (wywiadu), analiza kryminalna składa się z nieodzownych etapów postępowania ze zgromadzonym zasobem informacji (materiałem sprawy). Można je wyodrębnić w ustalonej kolejności pomimo płynnego przechodzenia przez te etapy czynności analitycznych i ich wzajemnego przenikania

Zapoznanie z materiałem i selekcja materiału

Pozornie sam fakt zapoznania się z materiałem zgromadzonym w sprawie ma prozaiczne znaczenie stanowiąc tło analizy. Jednak należy zauważyć szczególny charakter oglądu sprawy, co wynika z samej natury analizy, a więc wnikliwego czytania i rozkładania faktów na czynniki pierwsze. Aby rozpocząć czynności związane z porządkowaniem i selekcją materiału należy zapoznać się z całością. Dotyczy to zarówno zapoznania się ze wszystkimi kartami akt sprawy, jak i odtworzenia danych zawartych na innych nośnikach (zdjęcia, bilingi telefoniczne, wyciągi bankowe). Wstępne zapoznanie się z materiałem całościowym daje gwarancję dobrego zaplanowania kolejnych czynności analitycznych. Pozwala też na ocenę materiału pod kątem jego kompletności, wiarygodności (w odniesieniu do źródeł i jakości informacji), stopnia skomplikowania. Zasadą jest, by rozpocząć analizę od co najmniej jednego zapoznania się ze sprawą bez jednoczesnego rozpraszania uwagi na tzw. „obróbkę" materiału (notatki, selekcjonowanie itp.). Każde następne czytanie pozwala już na właściwą systematyzację oraz rozpoczęcie kolejnego etapu, jakim jest selekcja. Materiał, który trafia do analizy, przepełniony jest danymi różnego rodzaju, one zaś, stanowiąc nieuporządkowane fakty, wymagają segregacji. Po zapoznaniu się z materiałem należy go „oznakować", tj. wydzielić dane, które będą poddane dalszej analizie. Zdecydowana większość materiału zgromadzonego w ma charakter mało merytoryczny. Wynika to ze specyfiki konkretnych dokumentów/



Rys. 11. Etapy czynności analitycznych (źródło: opracowanie własne)

nośników (np. notatka, protokół przesłuchania świadka, zapis z monitoringu), gdzie niewielką część lub zawartość stanowi źródło danych przekładających się na jakąkolwiek wartość informacji. Można zaryzykować stwierdzenie, że tylko niewielka część materiału w sprawie jest wartościowa (w kontekście przydatności w dalszej analizie). Pozostała część to tekst, który jest swoistym tłem. Wystarczy przykładowo wskazać, że w protokole przesłuchania świadka niejednokrotnie zwraca się uwagę tylko na kilka akapitów, pozostała treść niczego nie wnosi. Podobnie większość z zabezpieczonej w danej sprawie dokumentacji nie będzie brana pod uwagę, również stenogramy rozmów telefonicznych w przypadku zastosowanego podsłuchu będą jedynie w wąskim zakresie zawierały informacje przydatne w analizie. Sposoby selekcjonowania mogą przybierać różną formę w zależności od indywidualnego warsztatu analityka. Praktycznym jest pracować na kopii materiału ze względu na swobodę pracy z tekstem w przypadku dokumentacji papierowej, na której można nanosić notatki, zaznaczać wybrane fragmenty, akapity czy też pojedyncze zdania. Przydatnym sposobem pracy z materiałem, pozwalającym na prostsze prześledzenie go w przypadku ponownego odczytu, jest używanie kolorów. Wyszukiwanie osób, pojazdów, adresów, czy nazw firm w tekście jest łatwiejsze, gdy dobierze się dla nich odrębną barwę i dokona zakreśleń. W przypadku pracy na oryginale stosować można kartki samoprzylepne z właściwym zapiskiem. Najbardziej efektywną pracę z materiałem (nie tylko w trakcie selekcji) uzyska się w przypadku dokumentacji elektronicznej. Digitalizacja materiału stała się już nieodłącznym elementem każdej analizy kryminalnej, dokonywana jest jednak głównie na wyselekcjonowanym już materiale, a nie na całości. Współcześnie coraz więcej danych przybiera formę elektroniczną, a to sprawia, że analityk ma do dyspozycji taką właśnie postać we wszystkich etapach analizy, co stanowi niewątpliwie jej atut. Poddany selekcji materiał podlega dalszej systematyzacji, którą można nazwać grupowaniem.

Grupowanie i scalanie

Wyselekcjonowanie danych z całości materiału przyśpiesza ich interpretację i skraca czas zapoznawania się z nimi. Dane te jednak nadal stanowią zbiór nieusystematyzowany, wymagający pogrupowania. Proces „szufladkowania" danych bądź informacji (jako wyniku przetworzenia i interpretacji i danych) jest czymś naturalnym w analizie kryminalnej (jak też w każdej innej analizie materiału). Przebiega jednak nieszablonowo, wynika z charakteru wyselekcjonowanego materiału i autonomicznej decyzji analityka kryminalnego. Łączyć można zarówno dane, informacje o konkretnej osobie, jak i o grupie osób, wszystkie informacje o firmie lub z podziałem na obieg dokumentacji, usługi transportowe, powiązania klienckie itd. Grupowanie danych i informacji w aplikacji bazodanowej, będącej narzędziem pracy analityka, polega na utworzeniu rekordów obiektów i połączeń. Obiektami będą np. osoba, rachunek bankowy, telefon (numer abonencki), zdarzenie, dokument, adres, firma i wiele innych wynikających ze specyfiki zagadnień w sprawie. Połączenia przybierają postać charakterystycznych relacji np. typu: znajomość, powiązanie kapitałowe, rozmowa telefoniczna, przelew bankowy, właściciel, użytkownik, abonent itd. Materiały poddane selekcji jednocześnie zasilają bazę danych, w której będą już posegregowane na typy obiektów i połączeń, a także pozwalają poprzez funkcjonalności analityczne oprogramowania na szybkie

tworzenie zbiorów. Te z kolei są wynikiem procesu myślowego analityka „odpytującego" bazę danych pod kątem określonych kryteriów. Taka czynność stanowi już pomost pomiędzy grupowaniem a scalaniem. Procesy selekcji i grupowania są najdłuższymi etapami czynności analitycznych i mogą zajmować zdecydowaną większość czasu przeznaczonego dla analizy. Jednak stanowią one fundament dla dalszych czynności analitycznych, które byłyby ułomne i nierzetelne w przypadku błędów popełnionych we wcześniejszych etapach. Analityczny rozbiór materiału na „czynniki pierwsze", wyselekcjonowanie danych istotnych dla analizy i ich pogrupowanie pozwala na ich późniejsze zespolenie. Przejście pomiędzy grupowaniem danych i ich scalaniem jest bardzo płynne, więc trudno nakreślić tu jednoznaczną granicę. Scalenie następuje w wyniku pogrupowania danych i informacji, a następnie ich zestawienia według obranych kryteriów. Może przybrać postać graficzną zgodnie z opisywanymi wcześniej technikami analitycznymi. Analityk, dysponując danymi i informacjami z różnych źródeł, może je opracować zgodnie z wytycznymi (celami analizy wskazanymi w zleceniu) oraz według własnych ustaleń i pomysłów. Kreatywność analityka może okazać się drogą do sukcesu analizy, zwłaszcza w pracy na materiale, w którym w sposób klasyczny nie jesteśmy w stanie zauważyć wszystkich zależności, nawet posiadając umiejętność tzw. „czytania pomiędzy wierszami". Z punktu widzenia taktycznego warto obrać kierunek scalenia materiału i zestawiania danych przez pryzmat występujących w sprawie powiązań oraz chronologii zdarzeń. Takie zespolenie pozwala uzyskać właściwy obraz sprawy, pójść w kierunku kolejnych zestawień (również technik analitycznych, tabel statystycznych), które stanowić będą podstawę procesu wnioskowania. Scalanie danych odbywa się poprzez wnikliwe studiowanie pogrupowanych informacji, diagramów, zestawień, a jego efektem jest utworzenie przesłanek.

Tworzenie przesłanek, opracowanie wniosków, zalecenia

Przesłanki stanowią istotny element wnioskowania, wpływają na kształt finalny analizy. Analiza kryminalna kończy się wnioskami i zaleceniami, te zaś muszą znaleźć uzasadnienie w materiale. Zbiór pogrupowanych faktów składających się na wnioski końcowe analityk prezentuje w postaci sprawozdania pisemnego bądź ustnego, gdzie kolejno proces analityczny, logiczne rozumowanie musi znaleźć odzwierciedlenie. Drogowskazem są tu przesłanki, które wynikają z zawartości merytorycznej materiałów, wiążą fakty zgodnie z przyjętym wcześniej pogrupowaniem (danych, informacji). W analizie kryminalnej przesłanka (w formie zdania lub kilku zdań) jest podsumowaniem zbioru faktów zawartych w poszczególnych grupach danych i informacji. Stanowczo przesłanki nie mogą przeobrazić się w „małe" wnioski. Stanowiłoby to zburzenie fundamentów wnioskowania, gdyż wniosek (traktowany w analizie kryminalnej jako wersja zdarzeń) nie może opierać się na innych pomniejszych wnioskach. Przesłanki decydują o późniejszej konstrukcji wniosków końcowych z przeprowadzonej analizy kryminalnej, a te mogą przybrać już postać np. wersji śledczej, konkluzji czy prognozy kryminologicznej. Wniosek należy traktować jako produkt analizy. Skojarzenie z działaniami marketingowymi jest tu jak najbardziej uzasadnione, gdyż uzyskiwanie akceptacji rezultatu pracy analityka przez odbiorcę analizy można by nazwać nieelegancko „sprzedażą wyniku analizy". Jeżeli owocem pracy analityka są wnioski, na podstawie których dana sprawa ma nowe oblicze, to niezwykle istotny jest sposób konstrukcji tych wniosków, ich wyjaśnienia (m.in.

przedstawienia scenariuszy), zastosowania właściwej argumentacji, wreszcie przekonania odbiorcy analizy kryminalnej. Nawet najlepiej wykonana analiza kryminalna może stracić na znaczeniu, jeżeli prezentacja wniosków (również procesów myślowych, które do nich doprowadziły) będzie niewłaściwa, potraktowana powierzchownie czy wręcz wypaczona. Wówczas wnioski i zalecenia mogą „skończyć na drugim planie" kolejnych działań. Wnioski w analizie kryminalnej opierają się na przesłankach, wynikają z nich i z nimi korespondują, rzucają też nowe światło na sprawę (hipoteza, prognoza śledcza). Przesłanki pełnią rolę popierającą wniosek, stanowią punkt wyjścia procesu wnioskowania. Wnioskowanie w analizie kryminalnej nawiązuje do powszechnych założeń logiki i jest przejawem logicznego rozumowania. Jak każda hipoteza, by została dowiedziona, musi przejść weryfikację. Korelacja pomiędzy wnioskami, a przesłankami w przypadku analizy kryminalnej sprowadza się również do odpowiedniego doboru słów w procesie konstrukcji zarówno przesłanek jak i wniosków.

Wnioski powinny odpowiadać na 7 złotych pytań kryminalistyki[30], by były w pełni wyczerpujące, jeśli analizowany materiał na to pozwala. Ich budowa zależy od tego, jaka forma prezentacji (pisemna, ustna) zostanie w danym momencie użyta. Najczęściej analitycy kryminalni poprzestają na sprawozdaniu pisemnym z analizy. Wnioski przybierają wówczas najczęściej postać zdań zgrupowanych w podpunktach. Podczas ustnego prezentowania wyników, wnioski powinny być zaakcentowane w taki sposób, by zachowały się w pamięci odbiorców jako istota analizy. Efektu tego można nie uzyskać w przypadku stosowania zdań nazbyt rozbudowanych, naszpikowanych zbędną treścią, należy więc pamiętać, że prezentacja wyników analizy kryminalnej nie jest okazją do przemówień. Na podstawie wniosków analityk przygotowuje zalecenia, które są równie ważnym produktem finalnym każdej analizy kryminalnej. Należy pamiętać, że zalecenia to nie polecenia. Analityk proponuje dalsze działania, ukierunkowuje je, w związku z tym zalecenia należy traktować jako rekomendacje, propozycje, wskazówki dla kolejnych czynności. Pomimo braku władczego charakteru zaleceń nie można stwierdzić, że są niezobowiązujące. Każda sprawa zlecana jest analitykowi z jakiegoś powodu (problemu, zagadnienia), zalecenia mają więc wytyczyć drogę rozwiązania problemów leżących u podstaw wcześniejszej decyzji o zleceniu. Zatem odrzucenie lub niezastosowanie się do sugestii analityka musiałoby wynikać z jakiejś istotnej przyczyny (np. spływ nowych informacji transformujących poprzednie ustalenia).

Zalecenia powinny zawierać słowa niekategoryczne: „należałoby", „wskazane jest", „rozważyć należy" etc. Przy ich formułowaniu należy unikać zwrotów kojarzonych z poleceniem bądź ujmowania ich w trybie rozkazującym np.: „wykonać", „przesłuchać", „uzupełnić", gdyż te mogą zrazić do analityka (ma on być uznawany za partnera a nie z osobę kontrolującą, kojarzony z dobrą współpracą, a nie z wytykaniem ewentualnych błędów).

Zalecenia, choć zamykają etapy czynności analitycznych, tworzone są w trakcie niemalże całego procesu analitycznego, niektóre na bieżąco konstruowane jako przemyślenia analityka, a zdefiniowane (lub reasumowane) na końcu, gdy wszystkie czynności zostały już wykonane. Zwieńczeniem czynności analitycznych będzie zaprezentowanie wyników analizy.

[30] 1) Co?; 2) Gdzie?; 3) Kiedy?; 4) W jaki sposób?; 5) Za pomocą czego?; 6) Kto?; 7) Dlaczego?, M. Kulicki, V Kwiatkowska-Darul, L. Stępka, *Kryminalistyka. Wybrane zagadnienia teorii i praktyki śledczo-sądowej*, Toruń 2005, s. 47.

Wykorzystanie analizy kryminalnej w podmiotach systemu bezpieczeństwa państwa

Podmioty odpowiedzialne za bezpieczeństwo państwa, realizując określone ustawowo zadania, wykorzystują szereg instrumentów, m.in. o charakterze prawnym, organizacyjnym czy też technicznym. Jednym z takich instrumentów jest analiza kryminalna, która wdrażana w szeregu podmiotach, w jednych ewoluowała w różnych kierunkach ich aktywności, w innych zaś nie znalazła większego uznania, co nie znaczy, że nie ma w tych ostatnich komórek analitycznych, które – odpowiednio „zmotywowane" – mogą okazać się jednak przydatne w pracy danego podmiotu.

Policja, jako prekursor analizy kryminalnej w Polsce

Pierwszą służbą w Polsce, która w sposób systemowy wprowadziła do swojej pracy i struktur analizę kryminalną była Policja. Wzorce czerpano z policyjnych doświadczeń państw europejskich jeszcze na długo przed akcesją Polski do Unii Europejskiej. Działania związane ze zwalczaniem przestępczości zorganizowanej i narkotykowej wpłynęły na wypracowanie standardów unijnych dotyczących wyposażenia technicznego oraz procedur w zakresie gromadzenia, przetwarzania i wymiany informacji krajów członkowskich.

Za narzędzie spełniające powyższe wymagania uznano brytyjski system wywiadu i analizy kryminalnej o nazwie Alert. W 2000 r. Komendant Główny Policji zatwierdził „Program wdrażania analizy kryminalnej", który zawierał główne założenia przyszłego funkcjonowania analizy kryminalnej w Polsce. Priorytetem strategii wdrażania było przygotowanie odpowiedniego zaplecza kadrowego, inwestycyjnego i organizacyjnego do uruchomienia systemu wywiadu i analizy kryminalnej Alert. System ten miał umożliwić Policji krajową i międzynarodową wymianę informacji w jednolitych standardach oraz współpracę przeszkolonych analityków kryminalnych, posługujących się tymi samymi metodami, technikami analitycznymi i narzędziami informatycznymi, podczas prowadzenia działań na terenie kraju i poza jego granicami[31].

Wskazane w przedmiotowym programie działania zmierzały do realizacji trzech zazębiających się obszarów: szkoleniowego (uzyskanie pożądanego zaplecza kadrowego), inwestycyjnego (zakup sprzętu i oprogramowania) i organizacyjnego (stworzenie struktur oraz regulacji prawnych umożliwiających powołanie i sprawne funkcjonowanie komórek analitycznych umocowanych w ramach wywiadu kryminalnego)[32]. Wdrażanie analizy kryminalnej w Policji odbywało się w tych trzech płaszczyznach jednocześnie.

Obszar szkoleniowy

W 1996 roku, a więc jeszcze przed omawianym programem wdrażania analizy kryminalnej, w Londynie została przeszkolona pierwsza grupa 10 analityków. Od 2000 roku rozpoczęto szkolenia we współpracy z Unią Europejską, które prowadzono w Centrum Szkolenia Policji w Legionowie. W ramach twinningu'98, na dwóch kursach przeszkolonych zostało 24 analityków

[31] Raport. nt. Analiza Kryminalna, Stan Aktualny i Plany Rozwoju, Biuro Służby Kryminalnej KGP, 2003.

[32] M. Hausman, *Implementation and development of criminal analysis in the polish Police*, [w:] *Crime Intelligence RiskAssessment & Intelligence LedPolicing*, CEPOL..., op. cit., s. 30.

operacyjnych, spośród których eksperci Unii Europejskiej wyłonili 6 kandydatów na polskich szkoleniowców. W 2001 roku odbyło się szkolenie 13 kandydatów na analityków operacyjnych z udziałem ekspertów unijnych, które jednocześnie prowadzone było przez wytypowaną szóstkę wykładowców. Łącznie liczba przeszkolonych analityków operacyjnych (przy udziale ekspertów UE) wyniosła na koniec 2001 r. 31 osób. W międzyczasie w ramach programów twinningowych szkolono kadrę kierowniczą z zakresu zarządzania analizą kryminalną.

Zgodnie z „Harmonogramem zaleceń wynikających z porozumienia bliźniaczego Twinning '98" uruchomiono centralny ośrodek szkolenia analityków kryminalnych w Wyższej Szkole Policji w Szczytnie. W 2001 roku przystosowano na potrzeby polskiej Policji materiały dydaktyczne UE (oparte na doświadczeniach ze szkoleń prowadzonych przez szkoleniowców z Wielkiej Brytanii), na podstawie których przygotowano program szkoleniowy analityków operacyjnych. W tym samym roku uruchomiono pierwsze szkolenie pilotażowe, a od 2002 r. rozpoczęto cykliczne szkolenia prowadzone wyłącznie przez polskich wykładowców[33]. W każdym przedsięwzięciu szkoleniowym, trwającym cztery tygodnie, oprócz wykładowców WSPol uczestniczyli również analitycy kryminalni z jednostek terenowych. Ich udział w szkoleniu miał na celu przekazywanie doświadczeń zebranych w trakcie wykonywanych analiz operacyjnych, co do chwili obecnej jest praktykowane.

Każdego roku w WSPol odbywa się kilka cykli szkoleniowych również z udziałem służb spoza Policji, przede wszystkim Straży Granicznej i Agencji Bezpieczeństwa Wewnętrznego, które rozpoczęły szkolenia swoich funkcjonariuszy od 2003 roku. W późniejszym czasie funkcjonariusze m.in. Służby Kontrwywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Służby Celnej oraz pracownicy prokuratury skorzystali z rozwiązań policyjnych i policyjnej bazy szkoleniowej.

Już od 2001 roku szkoleniem objęci byli nie tylko analitycy kryminalni, ale także kadra wyższego i średniego szczebla oraz pozostali policjanci, głównie pionów kryminalnych i dochodzeniowo-śledczych. Szkolenia te miały początkowo na celu rozpropagowanie idei analizy kryminalnej, ale przede wszystkim możliwości wykorzystania warsztatu analityka kryminalnego w prowadzonych sprawach. W październiku 2002 roku, dla podniesienia efektywności wewnętrznej wymiany informacji i doświadczeń, zorganizowane zostało Ogólnopolskie Sympozjum Analityków Kryminalnych, które nabrało cyklicznego charakteru i każdego roku organizowane jest w Wyższej Szkole Policji w Szczytnie.

Szkolenia analityków policyjnych odbywają się do dziś systematycznie w WSPol. Podobnie niezmiennie, choć stanowi to odrębną kwestię, formował się nabór kandydatów na analityków kryminalnych i skierowanie ich na omawiane szkolenia. Selekcja kandydatów stanowiła istotne zagadnienie od zainicjowania procesu wdrażania analizy kryminalnej, jej szczegóły zawarte zostały w wewnętrznych przepisach policyjnych, a na ich podstawie została implementowana do innych służb.

[33] J. Nęcki, *Analiza kryminalna. Stan aktualny i perspektywy*, [w:] *Policja Europy w XXI w. – w kierunku jakości. Materiały pokonferencyjne*, A. Letkiewicz i W. Pływaczewski (red.), Szczytno 2003, s. 119 i n.

Obszar inwestycyjny

W roku 1997, realizując przyjęty standard, nabyte zostały dwa rozwiązania sprzętowo- programowe w celu przetestowania ich przydatności dla Policji. Zakupiono pięć Samodzielnych Stanowisk Analizy Kryminalnej – SSAK (z oprogramowaniem analitycznym Analyst's Notebook firmy i2), w które wyposażono cztery jednostki terenowe oraz WSPol w Szczytnie.

Ponadto, zgodnie z założeniami „Programu wdrożenia analizy kryminalnej w jednostkach Policji", zrealizowano proces przystosowania systemu do wymagań użytkownika polskiego, w zakresie:

- dostosowania systemu do polskiego prawa i wymagań polskiej Policji,
- opracowania polskiej wersji językowej oprogramowania.

Zmodyfikowano także ówczesne rozwiązania sprzętowo-programowe systemu Alert z centralną instalacją systemu w byłym Biurze dw. z Przestępczością Zorganizowaną KGP. W 2003 roku – w ramach unijnego funduszu przedakcesyjnego Phare 2000 zakupione zostało wyposażenie dla ogólnopolskiego systemu wywiadu i analizy kryminalnej.

W kolejnych latach kierunkiem inwestycyjnym było zaopatrzenie jednostek terenowych w stanowiska dostępowe uruchomionego systemu oraz zapewnienia możliwości pracy na samodzielnym stanowisku zwiększającej się liczbie przeszkolonych analityków (początkowo zmuszeni byli dzielić między sobą stanowiska analityczne). W 2010 roku Policja dysponowała ponad 200 Samodzielnymi Stanowiskami Analizy Kryminalnej. Obecne inwestycje zmierzają do utrzymaniu potencjału wyposażenia stanowisk analitycznych, aktualizacji oprogramowania analitycznego. Jednakże w niektórych jednostkach nadal istnieje realne zapotrzebowanie na zwiększenie liczby stanowisk analitycznych.

Obszar organizacyjny

Wdrożenie analizy kryminalnej w działaniach Policji, a następnie szeroko rozumianego systemu wywiadu kryminalnego musiały być poprzedzone odpowiednimi zabiegami organizacyjnymi. Było to postępowanie wieloetapowe, które wymagało określonych zabiegów legislacyjnych i strukturalnych.

Priorytetem było, aby wszystkie jednostki organizacyjne Policji, przewidziane do realizacji zadań analitycznych, powołały komórki analizy kryminalnej. Po 2000 roku organizacja tych komórek przebiegała niejednolicie. Tworzone były pojedyncze stanowiska, niekiedy zespoły analizy kryminalnej.

Do 2003 roku przygotowano komórki analizy kryminalnej do włączenia w proces wywiadu kryminalnego (zgodnie z zaleceniami Unii Europejskiej) w następujący sposób:

1) we wszystkich jednostkach przewidzianych do realizacji zadań analitycznych powołano komórki analityczne,
2) komórki analityczne uzyskały charakter interdyscyplinarny,
3) wyodrębniono organizacyjnie komórki analityczne, w aspekcie ich przyszłej roli w funkcjonowaniu wywiadu kryminalnego.

Takie właśnie przygotowanie organizacyjne komórek analizy kryminalnej do funkcjonowania w procesie wywiadu kryminalnego pozwoliło uzyskać określone korzyści. Wyodrębnienie organizacyjne umożliwia komórkom analizy kryminalnej realizację zadań analitycznych

na rzecz całej Policji, a nie poszczególnych wydziałów czy służb. Interdyscyplinarność sprzyja realizacji zadań analitycznych w zakresie różnych rodzajów przestępczości, natomiast powołanie komórki koordynującej i nadzorującej działania w zakresie analizy kryminalnej pozwala na zachowanie jednolitości i spójności funkcjonowania oraz rozwoju analizy kryminalnej w procesie wywiadu kryminalnego, jak również reprezentowania jej na zewnątrz bezpośrednio lub poprzez inne komórki.

Analiza kryminalna nie mogła być zupełnie odosobnionym elementem pracy Policji, jej prawidłowe funkcjonowanie bowiem było, jest i zawsze będzie z osnową prawną i organizacyjną. Bez właściwego ugruntowania systemowych rozwiązań skazana byłaby na porażkę. Wskazać jednak należy, iż rozwiązania te nie były jednorodne, ewoluowały tworząc współczesny obraz analizy kryminalnej w Policji.

Straż Graniczna i Krajowa Admistracja Skarbowa

Straż Graniczna

W myśl zapisów ustawowych[34] Straż Graniczna (SG) jest jednolitą, umundurowaną i uzbrojoną formacją przeznaczoną do ochrony granicy państwowej, kontroli ruchu granicznego oraz zapobiegania i przeciwdziałania nielegalnej migracji.

Po przystąpieniu Polski do strefy Schengen, na Straż Graniczną nałożono obowiązki polegające przede wszystkim na ochronie zewnętrznej granicy Unii Europejskiej z Federacją Rosyjską, Ukrainą, Białorusią i w międzynarodowych portach lotniczych, jak też prowadzenie działań związanych ze zwalczaniem nielegalnej migracji na terytorium RP[35].

Głównym zadaniem Straży Granicznej jest zatem ochrona granicy „zielonej" i kontrola ruchu na przejściach granicznych, ale nie są to jej jedyne obszary działalności. Szeroki zakres zadań nałożonych na tę formację przewiduje m.in. rozpoznawanie, zapobieganie oraz wykrywanie przestępstw i wykroczeń, a także ściganie ich sprawców (zgodnie z właściwością przypisaną SG), jak również gromadzenie i przetwarzanie informacji, zwłaszcza z zakresu ochrony granicy państwowej, kontroli ruchu granicznego, zapobiegania i przeciwdziałania nielegalnej migracji oraz udostępnianie ich właściwym organom państwowym. Tym samym nałożone na SG zadania są w części charakterystyczne dla działań wywiadowczych, zmierzają zatem w kierunku analizy informacji, również analizy kryminalnej.

W ramach przedsięwzięć analitycznych stosowanych w tej służbie, wykonywane są analizy strategiczne oraz kryminalne analizy operacyjne. Na szczeblu centralnym znajdują się dwa wydziały analityczne, które usytuowane są w odrębnych pionach, tj. Wydział Kryminalnej Analizy Operacyjnej w Zarządzie Operacyjno-Śledczym oraz Wydział Analiz w Sztabie Komendanta Głównego, w oddziałach terenowych znajdują się ponadto komórki analizy ryzyka[36].

[34] Ustawa z dnia 12 października 1990 r. o Straży Granicznej, (Dz.U. 1990 nr 78 poz. 462).

[35] Więcej na stronie internetowej MSW: https://www.msw.gov.pl/pl/aktualnosci/10301,Nowy-model- funkcjonowania-Strazy-Granicznej.html, stan z dnia 18 marca 2017.

[36] Zgodnie z wytycznymi KGSG analiza ryzyka to ogół czynności, które prowadzą do wyodrębnienia elementów, cech i struktury zjawisk oraz wzajemnych powiązań między nimi, dokonywanych w celu identyfikacji braków i niedoskonałości systemu ochrony i zarządzania granicą (na który w szczególności składa się ogół przedsięwzięć związanych z ochroną granicy, kontrolą ruchu granicznego i funkcjonowaniem formacji) oraz wskazania sposobów eliminacji lub ograniczenia ich wpływu na poziom realizacji zadań; elementami składowymi tej analizy jest ocena

Zgodnie z wewnętrznymi uregulowaniami Straży Granicznej[37] kryminalna analiza operacyjna (KAO) dzieli się na wspierającą, towarzyszącą i inicjującą.

– kryminalna analiza operacyjna wspierająca polega na doraźnym i jednostkowym wykonaniu analizy, zlecanej na różnych etapach spraw ewidencji operacyjnej lub postępowań przygotowawczych oraz przeprowadzanej dla ściśle zdefiniowanych celów odpowiadających określonemu etapowi sprawy ewidencji operacyjnej lub postępowania przygotowawczego,

- kryminalna analiza operacyjna towarzysząca polega na możliwie stałym wykonywaniu analizy zlecanej na podstawie jednego wniosku, który może być składany na różnych etapach spraw ewidencji operacyjnej lub postępowań przygotowawczych oraz przeprowadzanej z uwzględnieniem dynamiki danej sprawy ewidencji operacyjnej lub postępowania przygotowawczego,
- kryminalna analiza operacyjna inicjująca polega na wykonywaniu analizy na podstawie wszelkich dostępnych źródeł danych w celu zainicjowania nowych zainteresowań operacyjno-rozpoznawczych lub dochodzeniowo-śledczych.

Pomimo pewnych odmienności w nazewnictwie, kryminalna analiza operacyjna wykonywana jest w celach analogicznych jak w Policji, oparta jest na podobnym systemie szkoleń specjalistycznych[38], jednorodnym warsztacie pracy analityków, w efekcie czego produkty analityczne w tym zakresie nie różnią się w obu służbach[39].

Straż Graniczna dysponuje mechanizmami regulującymi zarządzanie informacją. Są to przede wszystkim stosowne przepisy, określające zasady pozyskiwania informacji (jawnych i niejawnych), jak również ich gromadzenie, przetwarzanie oraz udostępnianie. Wsparciem dla tych działań są dedykowane informatyczne zbiory bazodanowe, ułatwiające odpowiednie gromadzenie informacji, rozliczalność ich wykorzystania, a także odpowiednią ochronę. Każdy funkcjonariusz SG, uzyskujący informacje służbowe, zobligowany jest do ich udokumentowania, natomiast charakter informacji decyduje o tym, do jakiego zbioru informatycznego zostanie ona wprowadzona (np. informacje dokumentowane z odprawy granicznej, informacje operacyjne i inne).

zagrożeń i ocena ryzyka, Wytyczne Nr 189 Komendanta Głównego Straży Granicznej z dnia 29 września 2006 r. w sprawie prowadzenia analizy ryzyka w granicznych jednostkach organizacyjnych Straży Granicznej, (Dz. Urz. KGSG z 2006 nr 8 poz. 68).

[37] Zarządzenie nr 26 Komendanta Głównego Straży Granicznej z dnia 15 kwietnia 2013 r. w sprawie wykonywania przez Straż Graniczną kryminalnej analizy operacyjnej i elektronicznego przetwarzania informacji kryminalnych (Dz. Urz. KGSG z 2013, poz. 33).

[38] Część funkcjonariuszy analityków kryminalnych SG szkoliła się w WSPol w Szczytnie.

[39] § 12 Zarządzenia nr 26 KGSG stanowi, że w ramach KAO (Kryminalna Analiza Operacyjna – przyp. autora) analityk kryminalny powinien w szczególności: „1) przetwarzać kompleksowo informacje zgromadzone w materiałach będących przedmiotem KAO; 2) wykorzystywać informacje zgromadzone w Centralnej Bazie Danych Analizy Kryminalnej „Analityk" oraz innych dostępnych bazach danych; 3) stosować adekwatne do celu KAO metody i techniki analityczne oraz specjalistyczne oprogramowanie analityczne; 4) współpracować na bieżąco z kierującym wniosek o wykonanie KAO; 5) uzgadniać z kierującym wniosek własne inicjatywy w zakresie uzyskiwania dodatkowych materiałów źródłowych w celu uniknięcia powielania tych działań; 6) opracowywać raporty analityczne bądź inne formy przedstawiana wyników w sposób umożliwiający wytyczanie kierunków dalszych przedsięwzięć w analizowanych sprawach ewidencji operacyjnej oraz postępowaniach przygotowawczych", Zarządzenie nr 26 Komendanta Głównego Straży Granicznej z dnia 15 kwietnia 2013 r., op. cit.

Funkcjonariusze mający dostęp do zasobów bazodanowych wykorzystują informacje do spraw służbowych, również analitycy w ramach wykonywanych analiz mają określony dostęp do tych baz. W drodze dalszego ich przetwarzania powstają różnego rodzaju dokumenty, także analityczne, które agregują wiedzę wykorzystywaną na poziomie taktycznym (bieżące sprawy) oraz na poziomie decyzyjnym (strategicznym).

Produktami analitycznymi są raporty z wykonanych kryminalnych analiz operacyjnych (dokonywanych w pionie operacyjno-śledczym), analizy zjawisk (np. analizy przestępstw dokonywanych przez cudzoziemców), analizy ryzyka (np. dotyczące głównych tendencji, ryzyk identyfikowanych przez Straż Graniczną w danym roku, opracowywanych w Sztabie Komendanta Głównego SG). W przypadku analiz kryminalnych odbiorcami są kierujący sprawę do analizy, natomiast w przypadku analiz zjawisk, analiz ryzyka kierowane są one do kierownictwa SG. W celu zapoznania innych funkcjonariuszy jednostek terenowych, zgodnie z dyspozycją przełożonych i w zależności od charakteru materiału oraz potrzeb, są one dalej dystrybuowane np. materiały publikowane są na stronie intranetowej.

Krajowa Administracja Skarbowa

Zadania Krajowej Administracji Skarbowej (powołanej w 2017 r.[40]) powstałej w wyniku połączenia Służby Celnej, administracji podatkowej i kontroli skarbowej, określone zostały przepisami ustawy z 16 listopada 2016r. o Krajowej Administracji Skarbowej, które realizowane są w oparciu o komórki organizacyjne w urzędzie obsługującym ministra (właściwego do spraw finansów publicznych), izby administracji skarbowej, urzędy celno-skarbowe i urzędy skarbowe. Krajowa Administracja Skarbowa wykonuje swe zadania, podejmując odpowiednio czynności kontrolne, prowadząc postępowania przygotowawcze zgodnie z przepisami ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego[41], Kodeksu karnego skarbowego lub ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia[42], prowadząc postępowania celne, audytowe, podatkowe lub administracyjne.

Proces wdrożenia analizy kryminalnej miał miejsce w okresie funkcjonowania Służby Celnej i jako taki został opisany w niniejszym referacie.

Dotychczasowe działania o charakterze analitycznym skupiały się przede wszystkim na analizach ryzyka w poszczególnych obszarach zainteresowań Służby Celnej. Podobnie jak w Policji i w innych służbach, prowadzone przez Służbę Celną działania koncentrowały się na gromadzeniu i przetwarzaniu informacji, w których analiza (również analiza ryzyka) odgrywała istotną rolę. Służba Celna dotychczas nie wykorzystywała analizy kryminalnej w swych działaniach, co w znacznym stopniu obniżało możliwości zwalczania przestępczości, zwłaszcza paliwowej, narkotykowej, alkoholowej, tytoniowej, hazardowej, jak również w zakresie e-kontroli prowadzonej w sieci Internet. Z tego też powodu wzrosło zainteresowanie omawianej służby wdrożeniem analizy kryminalnej.

[40] Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz.U. 2016 poz. 1947).

[41] Kodeks postępowania karnego (Dz. U. z 1997 r. Nr 89, poz. 555, z późn. zm.).

[42] Ustawa z dnia 24 sierpnia 2001 r – Kodeks postępowania w sprawach o wykroczenia, (Dz. U. z 2001 nr 106 poz. 1148).

Powołany został decyzją Szefa Służby Celnej Zespół Zadaniowy ds. Wdrożenia i Funkcjonowania Analizy Kryminalnej w Służbie Celnej[43]. Opracowana została koncepcja wdrożenia analizy kryminalnej w Służbie Celnej, w której przedstawione zostały propozycje rozwiązań w zakresie wprowadzenia nowego mechanizmu analitycznego wspierającego działanie tej formacji. Ma on zapewnić zwiększenie, a następnie utrzymanie wysokiego poziomu wykonywania ustawowych zadań Służby Celnej w obszarach: rozpoznawania, wykrywania, zapobiegania i zwalczania przestępczości z zakresu pozostającego we właściwości rzeczowej Służby Celnej. Zastosowanie analizy kryminalnej, jako narzędzia wspierającego Służbę Celną, wpisuje się w proces zmian dostosowujących organy Służby Celnej do skutecznego zwalczania zagrożeń. Zapoczątkowany ma być także proces przebudowy struktury organizacyjnej komórek zwalczania przestępczości oraz zasad ich funkcjonowania, co ma zagwarantować dalszy wzrost efektywności realizowanych zadań[44].

Działania realizowane z wykorzystaniem analizy kryminalnej zostały nakreślone przez „Koncepcję wdrożenia i funkcjonowania analizy kryminalnej w Służbie Celnej", zgodnie z którą mają one przede wszystkim zapewnić:

- precyzyjne ukierunkowanie czynności kontrolnych prowadzonych przez komórki zwalczania przestępczości na podmioty i osoby mogące mieć związek z działalnością przestępczą,
- dostarczenie informacji wymagających dalszego pogłębienia i potwierdzenia, np. w wyniku zastosowania obserwacji na podstawie art. 75b ustawy o Służbie Celnej, oraz prowadzenia działań operacyjno-rozpoznawczych w oparciu o art. 75c tej ustawy,
- możliwość tworzenia i weryfikacji stawianych hipotez śledczych w prowadzonych przez funkcjonariuszy komórek dochodzeniowo śledczych postępowaniach przygotowawczych,
- naprowadzenie na konkretne zdarzenia o charakterze przestępczym, a także umożliwić identyfikację osób i grup przestępczych stojących za nimi, wskazać mechanizmy ich działania, jak również struktury, w jakich funkcjonują,
- współpracę z innymi służbami zaangażowanymi w zwalczanie przestępczości zorganizowanej. Nadmienić należy, że proces wdrożenia analizy kryminalnej w Służbie Celnej w większości opierał się na doświadczeniach i wiedzy Policji co pozwoliło na profesjonalne i właściwe podejście do tematyki we wszystkich obszarach. Począwszy od obszaru organizacyjnego – w szczególności roli i miejsca analityków kryminalnych w strukturach Służby Celnej, szkoleniowego poprzez właściwe określenie potrzeb i metod szkoleniowych oraz obszaru inwestycyjnego – dobranie odpowiedniego wyposażenia sprzętowego i informatycznego. Współpraca zapoczątkowana przy wdrażaniu analizy kryminalnej w Służbie Celnej jest w chwili obecnej kontynuowana poprzez wspólne szkolenia zawodowe, seminaria i konferencje i wymianę doświadczeń co korzystnie wpływa na wysoki poziom wyszkolenia analityków kryminalnych. Taka współpraca przynosi wiele korzyści, począwszy od podnoszenia kwalifikacji analityków, poprzez unifikację „warsztatu pracy" co z kolei przekłada się na łatwość wymiany i przepływu informacji.

[43] Decyzja nr 18/SC Szefa Służby Celnej w sprawie powołania Zespołu Zadaniowego do prac związanych z wdrożeniem analizy kryminalnej w Służbie Celnej z dnia 6 listopada 2012 r.

[44] Koncepcja wdrożenia i funkcjonowania analizy kryminalnej w Służbie Celnej, dokument niepublikowany, 2013 r.

Rola analizy kryminalnej w służbach specjalnych

Wielowymiarowy i niezwykle silny wpływ na zapewnienie bezpieczeństwa państwa mają sprawnie funkcjonujące służby specjalne, których działania związane są ze zwalczaniem międzynarodowego terroryzmu, przestępczości zorganizowanej, proliferacji broni masowego rażenia i środków jej przenoszenia, a także z ochroną kontrwywiadowczą, bezpieczeństwem ekonomicznym państwa oraz ochroną informacji niejawnych. Tak szerokie spektrum zadań służb specjalnych wynika ze współczesnych zagrożeń bezpieczeństwa narodowego, wobec których należy postępować zarówno proaktywnie, jak i reaktywnie. Spoiwem łączącym aktywność służb specjalnych jest zapewnienie stałego wsparcia informacyjnego państwa zależnie od nakreślonych im zadań.

Służby te zdobywają, gromadzą i przetwarzają informacje dotyczące sfery bezpieczeństwa wewnętrznego i zewnętrznego (w bezpośrednim sąsiedztwie, przestrzeni europejskiej, euroatlantyckiej i globalnej) państwa polskiego. Odgrywają rolę w zabezpieczaniu polskich cywilno-wojskowych kontyngentów, które uczestniczą w misjach zagranicznych. Muszą na bieżąco rozpoznawać (analizować) sytuację w tych częściach świata, w których dochodzi do zamachów, konfliktów, napięć czy kryzysów (wewnętrznych lub międzynarodowych).

Celem sprawowania pieczy nad działalnością służb specjalnych RP powołane zostało przy Radzie Ministrów Kolegium do Spraw Służb Specjalnych, będące organem opiniodawczo-doradczym w sprawach programowania, nadzorowania i koordynowania działalności ABW, AW, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego oraz podejmowanych dla ochrony bezpieczeństwa państwa działań Policji, Straży Granicznej, Żandarmerii Wojskowej, Służby Więziennej, Biura Ochrony Rządu, Służby Celnej, urzędów skarbowych, izb skarbowych, organów kontroli skarbowej, organów informacji finansowej, jak również służb rozpoznania Sił Zbrojnych Rzeczypospolitej Polskiej.

W działaniach części służb specjalnych można wyróżnić takie czynności analityczne, które mimo swojej specyfiki pozwalają na zastosowanie analizy kryminalnej, zachowując jej uniwersalny charakter. Warto zatem zapoznać się ze specyfiką działań służb specjalnych, uwzględniając prowadzone przez nie czynności analityczne w kontekście stosowania (bądź dopiero możliwości wykorzystania) analizy kryminalnej. Jednocześnie istotnym zagadnieniem jest uwypuklenie tych rozwiązań, które w określony sposób ewoluowały w okresie stosowania analizy kryminalnej bądź też takich działań, które mogą być wykorzystane zamiennie w służbach RP. Służbami specjalnymi RP są: Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne.

Agencja Bezpieczeństwa Wewnętrznego (ABW)

Agencja Bezpieczeństwa Wewnętrznego została powołana Ustawą z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (obie te służby zastąpiły istniejący od 1990 r. Urząd Ochrony Państwa).

ABW – jako służba właściwa w sprawach ochrony bezpieczeństwa wewnętrznego państwa i jego konstytucyjnego porządku – ma najszerszy zakres zadań i obowiązków spośród pięciu służb specjalnych RP. Część z nich: kontrwywiad cywilny, zwalczanie terroryzmu na terytorium

RP, przeciwdziałanie proliferacji broni masowego rażenia i środków jej przenoszenia oraz ochrona informacji niejawnych w relacjach międzynarodowych – jest przypisanych wyłącznie tej Agencji.

W zakresie prowadzonych czynności Agencja Bezpieczeństwa Wewnętrznego realizuje działania: analityczno-informacyjne, operacyjno-rozpoznawcze, procesowe, w ramach systemu ochrony informacji niejawnych oraz wydaje opinie w stosownych sprawach. Swe zadania realizuje poprzez departamenty, biura, 16 delegatur oraz pozostałe jednostki organizacyjne.

Działania analityczno-informacyjne wykonywane przez ABW sprowadzają się do pozyskiwania oraz przetwarzania informacji istotnych dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, jak też międzynarodowej pozycji naszego kraju, a następnie przekazywane są one Prezydentowi i Premierowi RP oraz członkom Rady Ministrów. W 2012 r. raporty dotyczyły m.in.: zagrożeń godzących w podstawy ekonomiczne kraju; zagrożeń ze strony obcych służb specjalnych oraz kontrwywiadowczej ochrony strategicznie ważnych sektorów gospodarki narodowej; zagrożeń ze strony organizacji terrorystycznych, w tym nowych trendów w terroryzmie islamskim oraz środowisk i grup o charakterze ekstremistycznym; istniejących i prognozowanych zagrożeń bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, w tym wynikających z polityki zagranicznej i wewnętrznej państw, których cele strategiczne mogą kolidować z interesami Polski[45].

Wykonywanie przez ABW czynności operacyjno-rozpoznawczych jest ściśle związane z realizacją jej ustawowych zadań. Są to przewidziane prawem działania umożliwiające pozyskiwanie w sposób niejawny danych o osobach, miejscach lub zdarzeniach, mających znaczenie dla bezpieczeństwa wewnętrznego RP.

W ramach działań procesowych ABW zajmuje się wykrywaniem przestępstw szpiegostwa, terroryzmu, naruszenia tajemnicy państwowej i innych przestępstw godzących w bezpieczeństwo państwa, w podstawy ekonomiczne państwa, korupcji osób pełniących funkcje publiczne, w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym oraz ściganie ich sprawców. Funkcjonariusze ABW prowadzą także działania zmierzające do ustalenia miejsc pobytu sprawców przestępstw ukrywających się przed wymiarem sprawiedliwości.

Zakres działań Agencji jest ściśle powiązany ze zdobywaniem, gromadzeniem przetwarzaniem informacji. Uwidacznia się tu charakterystyczna dla tego typu służb rola analizy informacyjnej, dzięki której w możliwie szybki sposób dostarczana jest decydentom państwowym przetworzona informacja. Istotne jest także wykonywanie przez ABW analizy kryminalnej (w zakresie dotychczas opisywanym w niniejszej pracy), która trafiając na grunt czynności operacyjno-rozpoznawczych i procesowych w większości przypadków nie powinna odbiegać od tej stosowanej w Policji (np. sprawy „paliwowe").

[45] https://www.abw.gov.pl/pl/zadania/analizy-i-informacje/51,Analizy-i-informacje.html

Centralne Biuro Antykorupcyjne (CBA)

Korupcja w każdym państwie jest zagrożeniem dla praworządności, gospodarki, jak i całego systemu demokratycznego, należy przy tym do zjawisk wielopostaciowych i złożonych. Wymienione wyżej zjawisko, jak i inne realne zagrożenia bytu demokratycznego RP stały u źródeł decyzji o powołaniu odrębnej służby specjalnej. Centralne Biuro Antykorupcyjne powstało na mocy ustawy z dnia 9 czerwca 2006 r., która weszła w życie 24 lipca 2006 r.

CBA jest zatem służbą specjalną (jednocześnie centralnym urzędem administracji rządowej), która powołana została w celu zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, a także w celu zwalczania działalności godzącej w interesy ekonomiczne państwa.

Zasadniczym celem CBA jest zwalczanie korupcji pojawiającej się na styku sektora publicznego z prywatnym. Działania wykonywane przez CBA zawierają się w następujących obszarach:

- czynności operacyjno-rozpoznawcze oraz dochodzeniowo-śledcze,
- czynności kontrolne,
- czynności analityczne,
- prewencja antykorupcyjna (również edukacja antykorupcyjna)[46].

Centralne Biuro Antykorupcyjne, wykonując czynności analityczno-informacyjne, ukierunkowuje je na identyfikowanie nieprawidłowości i zagrożeń dla interesu ekonomicznego państwa, o wykryciu których zobligowane jest powiadomić Prezesa Rady Ministrów oraz inne osoby pełniące kluczowe funkcje w państwie. Zazwyczaj czynności te sprowadzają się do systematycznego monitorowania: zamówień publicznych, procesów prywatyzacyjnych oraz wybranych programów rządowych. Celem analizy będzie wstępne rozpoznanie potencjalnych zagrożeń oraz sporządzanie całościowej oceny sytuacji.

Ponadto CBA może uzyskiwać i przetwarzać dane ze zbiorów, w tym zbiorów danych osobowych, prowadzonych przez organy władzy publicznej oraz państwowe lub samorządowe jednostki organizacyjne[47]. W ramach prowadzonych czynności operacyjno-rozpoznawczych oraz dochodzeniowo-śledczych w CBA wykonywane są analizy kryminalne, których charakter nie odbiega od zadań przydzielonych analitykom Policji i niektórych innych służb.

Analitycy informacyjni usytuowani są w Departamencie Analiz i zajmują się głównie analizą strategiczną/systemową oraz wywiadowczą. Ich celem jest przede wszystkim identyfikacja istotnych zagrożeń korupcyjnych oraz godzących w interes ekonomiczny państwa. Poczynione w tym zakresie ustalenia przekazywane są do najważniejszych osób w państwie, wskazanych w art. 2 ust. 1 pkt 6 ustawy o CBA. W swojej pracy wykorzystują m.in. biały wywiad (OSINT), wewnętrzne i zewnętrzne bazy danych, informacje niejawne, a także warsztat analityków kryminalnych. Natomiast analitycy kryminalni usytuowani w delegaturach CBA zajmują się przede wszystkim analizowaniem materiałów przekazanych im przez zleceniodawców z pionów operacyjnych i śledczych (tzw. operacyjna i procesowa analiza kryminalna). Ich celem jest przede wszystkim wsparcie procesów decyzyjnych, które mają ukierunkować prowadzone w jednostkach CBA działania.

[46] https://cba.gov.pl/pl/o-cba/zadania/350,zadania.html

[47] Art. 22. Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2012 r. poz. 621).

Analiza kryminalna znajdzie zastosowanie wszędzie tam, gdzie przetwarza się dane masowe, w szczególności na rzecz zapewnienia bezpieczeństwa państwa. Dotyczy to zarówno problemów w skali mikro (analiza zdarzenia, sprawy), jak i makro (analiza strategiczna, systemowa). Jak wspomniano wcześniej, analitycy informacyjni CBA w ramach analiz strategicznych i wywiadowczych chętnie korzystają z warsztatu analityków kryminalnych. Taka kompilacja różnych, sprawdzonych metodologii podnosi znacznie efektywność działań.

Zakończenie

Organy władzy i administracji odpowiedzialne za bezpieczeństwo wewnętrzne stają przed dylematem związanym z podejmowaniem decyzji nie tylko w sprawach strategicznych, ale także i bieżących. Decyzje podejmowane są w oparciu o analizę informacji. Każdy z organów, mając swój indywidualny system gromadzenia, magazynowania i przetwarzania informacji, korzysta z wypracowanych wewnątrz, w ramach swoich struktur, praktyk w tym zakresie.

Analiza kryminalna, zapoczątkowana kompleksowo w Polsce przez Policję, nie tylko jest już stosowana przez większość podmiotów odpowiedzialnych za bezpieczeństwo państwa, ale jest też przez nie modyfikowana i dostosowywana do własnej specyfiki. Wprowadzane zmiany dowodzą, że następuje rozwój dotychczasowych rozwiązań. Do podmiotów już korzystających z instrumentów analizy kryminalnej, poza Policją, która jest jej głównym użytkownikiem, należą służby specjalne RP, które w pewnych obszarach stosują analizę kryminalną, a w innych korzystają z jej warsztatu. Ponadto kolejne podmioty takie jak Służba Celna i jej następca Krajowa Administracja Skarbowa, rozpoczynają kompleksowe wdrażanie analizy kryminalnej w swych działaniach. Możliwa jest również ewolucja i kompilacja różnych rozwiązań dotyczących stosowania analizy kryminalnej, tym samym też ich adaptacja w innych obszarach, w których dotychczas nie była stosowana np. przez służby specjalne przy realizacji czynności analityczno-informacyjnych oraz w procesie opracowywania strategicznych raportów. Mechanizmy analizy kryminalnej, mogą być także stosowane poza strukturami państwowymi, w sferze prywatnej, głównie przez banki i firmy ubezpieczeniowe, narażone na zagrożenia związane z funkcjonowaniem rynku finansowego i ubezpieczeniowego.

Istotnym kierunkiem szerszego wykorzystania analizy kryminalnej w przyszłości będą działania związane z gromadzeniem i przetwarzaniem dużej liczby informacji bez względu na ich charakter, również w podmiotach, które dotychczas nie stosowały analizy kryminalnej.

Naturalnym wydaje się także możliwość rozwoju analizy kryminalnej we wszelkich kierunkach, od szerszego jej wykorzystania w obrębie opisanych podmiotów, działających na rzecz bezpieczeństwa, po rozszerzanie wachlarza tychże podmiotów. Analiza kryminalna jest instrumentem, który nie tylko może być stosowany niemalże powszechnie, ale dość łatwo daje się modyfikować, dostosowywać do specyficznych potrzeb, nie tracąc przy tym nic ze swych wyjątkowych walorów.

Bibliografia

Analiza kryminalna (uaktualniona wersja 2.0.), przekład G. Butrym, Legionowo 1999.
Analiza kryminalna, opracowanie wewnętrzne (niepublikowane) KGP, Warszawa 2004.
Chlebowicz P. i Filipkowski W., *Analiza kryminalna aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2011.
Gołębiowski J., *Profilowanie kryminalne*, Warszawa 2008.
Hanausek T., *Kryminalistyka. Zarys wykładu*, Kraków 2000.
Hausman M., *Implementation anddevelopment of criminalanalysis in thepolish Police, [w] Crime Intelligence Risk Assessment & Intelligence Led Policing*, CEPOL, Warszawa 2010.
Hołyst B., Kube E., Schulte R., *Przestępczość zorganizowana w Niemczech i w Polsce. Zwalczanie i zapobieganie*, Warszawa 1998.
Huzior-Kamińska A., *Medycyna sądowa w służbie profilowania kryminalnego sprawców zabójstw*, [w:] J. Ignaczak W., Michna P., *Analiza kryminalna*. *Zarys wykładu*, Szczytno 2002.
Ignaczak W., *Wybrane zagadnienia analizy kryminalnej*, Szczytno 2005.
Informator o Centralnym Biurze Antykorupcyjnym, Warszawa 2012.
Instrukcja Stosowania Analizy Kryminalnej w Służbie Celnej.
Kobylas M. *Zastosowanie analizy kryminalnej w zwalczaniu cyberterroryzmu* – referat.
Kobylas M., Hausman M., *Problemy funkcjonowania analizy kryminalnej w Polsce w kontekście aktualnych rozwiązań i doświadczeń*. Sprawozdanie z III Sympozjum Analityków Kryminalnych (Szczytno, 8-10 listopada 2004 r.). „Policja", nr 4 z 2004.
Kulicki M., Kwiatkowska-Darul V, Stępka L., *Kryminalistyka. Wybrane zagadnienia teorii i praktyki śledczo-sądowej*, Toruń 2005.
Korzeniowski L. F., *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, Kraków 2008.
Olender-Skorek M., Wydro K. B., *Wartość Informacji, Telekomunikacja i Techniki Informacyjne*, tom nr 1-2/2007, Warszawa 2007.
Liedel K., *Profilowanie sprawców przestępstw terrorystycznych,* [w:] J. Konieczny, M. Szostak (red.)*, Profilowanie kryminalne*, Warszawa 2011.
Nęcki J., *Analiza kryminalna. Stan aktualny i perspektywy*, [w:] *Policja Europy w XXI* w. – *w kierunku jakości. Materiały pokonferencyjne*, red. A. Letkiewicz i W. Pływaczewski, Szczytno 2003.
Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2012 r., Warszawa 2013.
Raport. nt. Analiza Kryminalna, Stan Aktualny i Plany Rozwoju, Biuro Służby Kryminalnej KGP, 2003.

Źródła prawa

Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz.U. 2016 poz. 1947).
Ustawa z dnia 24 lipca 1999 r. o Służbie Celnej (Dz. U. z 1999 Nr 72, poz. 802).
Ustawa z dnia 24 sierpnia 2001 r – Kodeks postępowania w sprawach o wykroczenia, (Dz.U. z 2001 nr 106 poz. 1148).
Ustawa z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz.U. z 2009 r. Nr 168, poz. 1323).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553).

Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2012 r. poz. 621).
Zarządzenie nr 1012 KGP z dnia 23 września 2004 r. w sprawie stosowania przez Policję analizy kryminalnej (Dz. Urz. KGP z 2004 r. nr 20, poz. 124).
Wytyczne Nr 189 Komendanta Głównego Straży Granicznej z dnia 29 września 2006 r. w sprawie prowadzenia analizy ryzyka w granicznych jednostkach organizacyjnych Straży Granicznej, (Dz.Urz. KGSG z 2006 nr 8, poz. 68).
Zarządzenie nr 26 Komendanta Głównego Straży Granicznej z dnia 15 kwietnia 2013 r. w sprawie wykonywania przez Straż Graniczną kryminalnej analizy operacyjnej i elektronicznego przetwarzania informacji kryminalnych (Dz. Urz. KGSG z 2013, poz. 33).

Źródła elektroniczne

http://www.antykorupcja.gov.pl/ak/instytucje-antykorupcy/wyspecjalizowane/w-Polsce/
https://www.abw.gov.pl/pl/zadania/analizy-i-informacje/
http://analitycy.org/
https://cba.gov.pl/
http://www.wspol.edu.pl/d/archiwum/389-22-24-wrzepnia-miynarodowe-seminarium--analitykkryminalnych

Arkadiusz Pytlik

Silesian Customs and Revenue Office in Katowice

Criminal analysis in internal security services

Abstract

The presentation discusses advantages and versatility of criminal analysis as a modern tool for combating organised crime. It includes a brief discussion of the history of criminal analysis, the process of implementing criminal analysis in the Customs Service, definitions, status in the detective and evidence process as well as types of analyses. It also provides examples of visualisation of analysis findings in the form phone call billings, flows of goods, cash flows, chronology of events (charts with timelines), personal connections. It reviews the procedure of commissioning criminal analysis and rules of cooperation with the commissioning official. Finally, it gives examples of employment of criminal analysis by the Customs Service.

Introduction

Ensuring security is the primary function of every State. Implementation of key national interests of the Republic of Poland involves also actions of services responsible for national security. Efficient management of internal security is a resultant of the efficiency and effectiveness of actions taken by individual services and entities involved. It may largely depend on their ability to manage information held, and therefore on the quality of their analytical activities. The requirements imposed on services responsible for national security include efficient exchange of information, knowledge sharing, cooperation with other State agencies as well as activity on the international front. Analytical activities include a vast spectrum of issues, requiring not only a broad perspective of general matters but also specialised insights into narrow fields. Information analysis in service today is supported by *inter alia* criminal analysis, which has been present in Poland's services for more than a decade now.

Information analysis is a method that is employed in a number of areas. Its application in the context of events of interest to State services and other security entities is not a novelty. It is an important element that supports actions of law enforcement agencies, chiefly in its service provision capacity[1]. Practically every entity that executes security tasks employs analysis, but not every one of them does this in the identical manner. The main elements that differentiate the scope in which analysis is used include the remit as well as professional skills

[1] M. Hausman, M. Kobylas, *Problemy funkcjonowania analizy kryminalnej w Polsce w kontekście aktualnych rozwiązań i doświadczeń. Sprawozdanie z III Sympozjum Analityków Kryminalnych* (Szczytno, 8-10 listopada 2004r.), Policja 4/2004, p. 77.

and techniques of the analyst or a person who conducts analyses without formal qualifications. Employment of uniform techniques of working with information, use of analysis support tools and processing of information all have contributed to the evolution of criminal analysis towards wider applications. Many entities interested in police solutions have incorporated criminal analysis in their work, which shows that it is recognised as a universal method.

History of criminal analysis and Anacapa programme

Analysis as a classical process of thought has always been around. However, analysis in the context of unified analytical techniques is a contemporary phenomenon. In order to put the beginning of criminal analysis on a time scale it must first be appropriately defined. *Criminal analysis means identifying and making presumptions about links between data on criminal activities and other, potentially associated information to make them available for use by law enforcement agencies and courts. It involves identification or establishment, in as much an accurate manner as possible, of internal connections between information on a crime and all other data acquired from various sources, and use thereof for operational, investigative and strategic purposes. It is a recognised tool that supports detection processes*. Criminal analysis is a working method of the Police which, at its current stage of development, has taken permanent roots in the practice of the widely understood detection process. It is often an important element that supports actions of law enforcement agencies, chiefly in its service provision capacity[2].

The rapid growth of organised crime in the United States, covering a number of states and foreign territories, made it necessary to develop the „ANACAPA" scientific programme in the 1960s to support the police work. The programme became the starting point for development of analytical techniques and methods that have been in use in the USA to this day. The impulse to create a number of criminal intelligence tools, including the Anacapa scientific programme developed in the United States by Anacapa Sciences Inc., was provided by the aforementioned growth of organised crime. It was important, however, to make appropriate use of the analytical concepts developed and put them in practice in a uniform manner. The Anacapa programme became one of options offered to the intelligence training market and was quickly recognised in Europe.

Europe started introducing analytical methods and techniques based on US solutions in late 1980s. The British were the first to do so, soon followed by the Dutch. At present, police institutions in each European Union and Europol Member State work in accordance with uniform analytical standards. This solution significantly facilitates cooperation between police forces in combating cross-border and international crime of organised nature. Poland's accession to the European Union faced Polish Police and other internal security institutions with a number of new challenges. One of them was the need to establish relevant analytical structures that would meet the standards in place in other European Union Member States. The process of building such structures in Poland, based on the ANACAPA project, started in 2000. First training courses for Polish analysts were conducted by EU trainers. The original trainee analysts constituted

[2] M. Hausman, M. Kobylas, *Problemy funkcjonowania analizy kryminalnej w Polsce w kontekście aktualnych rozwiązań i doświadczeń. Sprawozdanie z III Sympozjum Analityków Kryminalnych* (Szczytno, 8-10 listopada 2004r.), Policja 4/2004, p. 77.

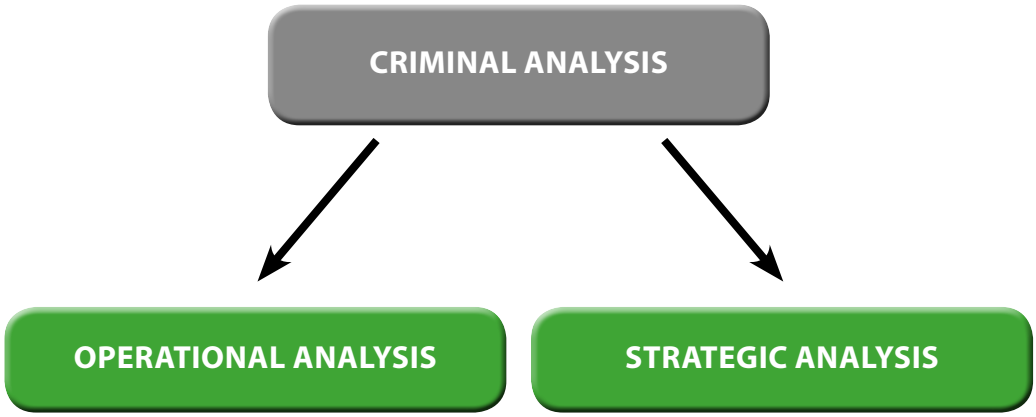


Figure 1: types of criminal analysis (source: own research)

the base on which the academic and educational personnel that could meet the modern day requirements was built in Poland. In the early days, there was the Delegated Team for Criminal Analyst Training operating within the Criminal Service Institute and then the Criminal Service Department. The existence of the dedicated criminal analysis group was formalised on 1 December 2004, and the group operates now as part of the Organised Crime and Terrorism Research Institute of the Police Academy in Szczytno[3], where initial and refresher training courses are provided to the Police force and personnel of other services like Border Guard[4], the Government Protection Bureau, the Internal Security Agency, the Central Anti-Corruption Bureau, the Military Counterintelligence Service, the Customs Service and prosecutor's offices.

It must be emphasised that criminal analysis is now among the most effective tools used by the Police, both in investigation and operational work. Criminal analysis employs uniform techniques for hypothesising, crime reconstruction, identification of other crimes related to the underlying crime, identification of criminal network structures and analysis of scope and methods of criminal activities[5].

Analysis, assessment and interpretation of information is an information processing activity based on logical and creative thinking aimed at producing findings (grounds for initiating further inquiries, investigations or operations) that permit further actions. In principle, police work is based mainly on information processing[6].

Classification and forms of criminal analysis

Similarly to the concept of criminal analysis itself, classification of criminal analysis can be presented in different ways across the world. The aforementioned British training model, based on which the assumptions for the Polish programme have been established (modified

[3] M. Kobylas, Application of criminal analysis to combating cyberterrorism – a research paper.

[4] A note from the author – after the initial training at the Police Academy in Szczytno, the Border Guard continue to train their criminal analysts at the Border Guard Training Centre in Kętrzyn.

[5] Analiza kryminalna (uaktualniona wersja 2.0.) / [przekł. Grzegorz Butrym]; Centrum Szkolenia Policji, p. 9.

[6] W. Ignaczak, *Wybrane zagadnienia analizy kryminalnej*, Szczytno, 2005, p. 9.

over the years, but with the historical core training framework maintained), divided criminal analysis into two types (Figure 1) – operational analysis and strategic analysis.

There is also the term „economic (financial) criminal analysis"[7] which refers to a comprehensive review, and interpretation, of all information (particularly financial and accounting information) related to specific businesses. It is aimed at searching for evidence of criminal activities in economic transactions. However, it seems unnecessary to distinguish another type, as the specific scope of actions in economic analysis falls within the scope of operational analysis, and only the subject of interest is different.

As already said, analytical actions, on their own, are universal regardless of what their subject is and what information is processed by the analyst.

Operational analysis

Operational analysis serves the achievement, in as short a period as possible, of an objective set by respective law enforcement agencies which is seizure or confiscation of the object of a crime. The adjective „tactical", which is sometimes used in conjunction with the term, can be found in the American literature, where it means examination of data aimed at answering the questions of where, when and how a specific crime was committed[8]. In Poland, the term „criminal analysis" is in fact equated with operational analysis[9]. This may be due to the fact that when criminal analysis was being introduced in the Police force, the main emphasis was on supporting the detection process with a view to fast, short-term and tangible results. Also other services, „peeping" on those results, decided to take a similar route and based responsibilities of their criminal analysts mainly on tasks that fall within the scope of operational analysis. Also, it must be highlighted that operational analysis does not encompass operational or exploratory activities only. Indeed, its spectrum includes all cases and all information gathered in the process as well as all data acquired by means of legally permitted methods of work.

Although the objectives set in the operational analysis definition presented above can be regarded as model ones, it should be remembered that they are just ones of many possible. Each separate case of operational analysis is different and may have different objectives. In the long practice of utilisation of criminal analysis by Poland's law enforcement agencies, such analyses have been aimed at various objectives like establishing or arresting the perpetrator, gathering evidence, setting out the routes of further operations, answering to specific questions asked by the party which commissioned a particular analysis or „just" compiling certain statistics and presenting relations between data (which is merely a small group of possible objectives offered by operational analysis).

Just like with listing of all objectives of operational analysis, it is pointless to enumerate all cases that can be „referred" to operational analysis. The need to conduct criminal analysis,

[7] W. Ignaczak, P. Michna, *Analiza kryminalna. Zarys wykładu*, Szczytno 2002, p. 6.

[8] Chlebowicz P. i Filipkowski W., *Analiza kryminalna aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2011, p. 42.

[9] Police and Border Guard internal regulations as well as official correspondence and training materials use also the terms „operational criminal analysis" or „criminal operational analysis".

or lack thereof, becomes evident only in the context of specific conditions of a case. When should a specific case be referred to criminal analysis? The ideal moment is when the officer in charge of the case becomes subjectively aware of his or her inability to handle the evidence material gathered. On the formal front, this depends on applicable internal regulations. For example, a Regulation of the Chief Commander of Police[10] lists a number of circumstances that give rise to employment of criminal analysis and enumerates the following case characteristics:

- multi-thread cases;
- cases covering a large territory;
- cases in which the *modus operandi* indicates high specialisation of the criminal activity;
- cases that have an evolutionary character.

Each of the aforementioned characteristics may be somehow problematic in terms of interpretation. The multi-thread character of a case may be interpreted in terms of numbers (a few, a dozen), so how many threads a case must have to subject it to analysis? The answer to this question is not rooted only in identification of the minimum number of all threads, but also in the nature of those threads. Apart from main threads, many cases have also secondary threads which need analysing as well. Certain threads are not very complicated, while some others are, and these elements sometimes determine the further course of action. Then, there is the issue of a large territorial coverage. Here, the definition is not clear either, as for one officer the term „large coverage" may mean an area that exceeds beyond the area of operations of his or her unit, while for some others it may mean the area of a Province etc. Further, there are cases where *the modus operandi* suggests a highly specialised manner in which the perpetrator or perpetrators operate. Criminals do not have licences or certificates to demonstrate their criminal skills (at best, they can use knowledge gained at universities, training courses etc.). Therefore, their level of criminal proficiency will be assessed discretionarily by a Police officer, who will judge it through his or her own professional experience.

Interestingly, all the characteristics referred to in the Regulation in question and discussed so far should be met cumulatively. An alternative appears in the passage about the evolutionary character of a case, which in itself is also very unclear and discretionary. Any case where investigative activities span over time (months, years) may be evolutionary, as may be one that covers an increasing number of interlinked individuals and events.

It may therefore be presumed that the author of these guidelines wanted only to underline the unique nature of criminal analysis, which in Police matters should be „reserved" mainly for „higher calibre", priority and multi-volume cases. Such interpretation results from the phrase „in particular..." that precedes the passage in question and suggests that the characteristics listed in the Regulation do not represent a closed catalogue, so it is possible to expand the scope to cases other than those specifically listed. The practice shows that also „minor" cases are referred, of course with due regard to the current workload of a given analytical unit. Therefore, it seems that every case where the officer in charge is convinced that criminal analysis is required should have an open way to such analysis, provided that the officer is not

[10] Regulation No. 1012 of the Chief Commander of Police of 23 September 2004 on employment of criminal analysis by the Police (Official Journal of the National Police Headquarters No. 20/124, 2004), §2.

mistaken in his or her judgement. Otherwise, lower level units which work less complicated cases might get discouraged to or even resign from using criminal analysis. Surveys, also ones regarding this issue, have showed this presumption to be true.

Contrary to the opinion that analyses are conducted mostly in criminal cases, one could recently notice an increase in the number of analysis referrals in typical economic cases, which can be understood given the increasingly complicated character of economic crime and complex networks of links in such crimes. While operational criminal analysis is the exclusive domain of criminal analysis units, strategic analysis is conducted by other analytical units depending on the target scope of the process.

Forms of operational analysis

All forms of operational criminal analysis share one common element – analytical activities focused on specific cases to achieve quick effects in accordance with the definitions provided above. Every form involves a specific analytical technique, or a set of techniques, which can be selected by a criminal analyst to match a specific case.

Classification criterion: the crime

Analysis of a case – it consists in reconstructing the course of a crime by establishing the chronology of successive or concurrent events in order to establish possible relations between the events, identify information gaps and inaccuracies in evidence, identify direction of further activities.

Techniques most often used in case analysis include chronological diagrams and other techniques, always selected on a case-by-case basis. Reconstruction of events provides for presenting a specific crime on a time scale and for organising the material gathered. In a standard configuration of a case file, sheets are added as they arrive – from the oldest to most recent depending on the date on which a particular document was created or received by the unit. As a result, the material gathered offers no logical sequence of events and the documents, and most importantly information, on file apply to different time periods, which brings chaos to the chronology of the events. It is therefore very easy to omit certain very important facts or inconsistencies in information and accounts of events. Visualisation of information in the form of a chronological diagram makes it possible to follow the sequence of facts as confronted against the rest of the material, thus facilitating an analytical look and fresh conclusions.

Comparative analysis of cases – it is conducted to establish, on the basis of information compiled from different cases, whether specific crimes were committed by the same perpetrator or perpetrators. As a result, the selected cases are linked and the evidence gathered thus far show a fresh picture and represents a larger group of information.

Serial criminals often operate in their own unique manner, thus largely increasing the chances of making errors. A unique *modus operandi*[11] may be observed in an individual or a group of individuals, less often an entity (a company). Analytical actions aimed at searching for a possible

[11] As defined by T Hanausek „it is a specific, characteristic and usually repeatable manner of behaviour of the perpetrator which reflects individual features, characteristics and capabilities of the person using this manner". Cf. T. Hanausek, Kryminalistyka. *Zarys wykładu*, Kraków 2000, p. 45.

serial nature of crimes consist in establishing the rules of selection according to which cases can be chosen for further comparison (based on characteristics of case „A", similar crimes are searched for in cases „B", „C", „D"..) from among either current or archive cases. Next, criteria are established for the comparison proper, i.e. for comparison of descriptive characteristics and exposure of analogous ones. There are situations where several crimes of the same type are committed and common features of all those situations are compared based on predefined criteria without any pre-selection (kidnappings in a specific area of Poland, hackers attacks, false bomb threats). On the occasion of serial crimes attention must be paid to a number of features like features of the perpetrator (e.g. physical, mental), features of the victim (the victimological aspect may be very important due to a possible pre-selection of victims by the perpetrator), features of the scene of the crime, the aspect of planning (preparation of the scene, tools, ambush, techniques aimed at deceiving law enforcement officers), the manner in which the perpetrator behaved at the crime scene (techniques and items used, method of communication, covering the traces, semantic analysis of communication) and others, depending on the type of a crime.

Classification criterion: the criminal

Analysis of crime groups – it is conducted to systematise the information in hand regarding a specific crime group in order to establish the group's structure and roles of individual members taking into account locations, objects (also economic entities) and means of transport relevant to the group. Groups can be organised or loosely linked, in which case a person plays a specific role (commits a crime) without any relation to the other members. When analysing crime groups, one must consider sociological conditions that govern functioning of individuals within a specific group, whether formal or informal, which are reflected also in the case of such groups. Even if the nature of a group is informal, it may adopt a number of operating principles characteristic of formal groups (e.g. military), where the leadership is strictly respected and orders rigorously executed (the leader achieves the status, recognition and respect within the group). Since secrecy is a key characteristic of organised crime groups[12], information held may not give a straightforward picture of a group's structure or roles of its members, but they may constitute the basis for drawing conclusions.

Analysis of crime groups (organised) should be aimed at establishing:

- hierarchical structure,
- specialisations and division of roles within the group members,
- antagonisms or collaboration with other groups,
- links with individuals (entities),
- international links,
- resources (tangible assets, logistics etc.).

Visualisation of the structure of a group will be significantly facilitated by a diagram of connections between individuals and objects and their roles and relations between them.

[12] B. Hołyst, E. Kube, R. Schulte, *Przestępczość zorganizowana w Niemczech i w Polsce. Zwalczanie i zapobieganie*, Warszawa 1998, p. 51.

An important element of such analysis is the ability to link facts and behaviours, frequently based on sketchy information. Not every evidence material provides an „A to Z" picture of the composition of a group and roles of its members, and it is the analyst's responsibility to systematise the knowledge, provided the he or she is commissioned with such task. Sometimes an apparently obvious network of links occurs to be more complicated on a thorough analysis of the material gathered. A lot depends on the ability to „read between the lines", which is an important skill of an analyst, who apart from the classic ability to link facts must also rely on his or her intuition, experience or independent acquisition of information (e.g. open source intelligence).

Specific profile analysis – it is an effort to establish traits of character of the perpetrator of a crime based on a description of that crime[13]. Preparation of psychological characteristics of a perpetrator requires the participation of an expert – a psychologist. Although it is not a common practice in Polish law enforcement agencies, one can nevertheless see an increased interest in this „service" within the Police force, especially in the case of dangerous and brutal crimes (e.g. homicides, rapes, arsons, acts of terrorism[14]). At present, the analysis in question should be linked with the process of criminal profiling, although the latter has a broader spectrum of interests. The scope of specific profile analysis significantly corresponds with the position of FBI agents, profiling pioneers, who define it as identification of the perpetrator's features based on analysis of the crime leading to a general profile of the individual[15]. Specialists who prepare characteristics of psychologically unknown persons are referred to as profilers. Although they have their own experience in criminal cases, they much more tend to rely on scientific foundations of profiling (criminal profiling in the case of perpetrators of crimes). The expert nature of criminal profiling is associated with the requirement to explore, among others, psychology, forensics, criminology, victimology, psychiatry, forensic medicine, sociology, sexology and even statistics[16]. This multidisciplinary nature of criminal profiling overlaps with the profiler's practical knowledge and intuition. Aimed at outlining personality, physical, social and other features (depending on a specific case), criminal profiling focuses on relations that link the perpetrator and the victim, the scene of the crime or establishing the motive[17], which is very important in subsequent detection activities (the motive may be unknown, the perpetrator may be diverting the law enforcement's attention to a false motive).

In line with the assumption made above, specific profile analysis falls within the scope of criminal profiling (which is a much broader concept), which in turn, in accordance with criminal analysis guidelines, particularly in the area of analytical reasoning, should be based

[13] Analiza kryminalna (uaktualniona wersja 2.0.)..., op. cit., p. 29.

[14] More in: K. Liedel, *Profilowanie sprawców przestępstw terrorystycznych*, [in:] J. Konieczny, M. Szostak (edit.), ibid, pp. 186-203.

[15] R.K. Ressler, J.E. Douglas, A.G. Burgess, R.L. Depue, Violent Crime, FBI Law Enforcement Bulletin 54 no. 8, 1985, [quote after:] J. Gołębiowski, *Profilowanie kryminalne*, Warszawa 2008, p. 8.

[16] More in: A. Huzior-Kamińska, *Medycyna sądowa w służbie profilowania kryminalnego sprawców zabójstw*, [in:] J. Konieczny, M. Szostak (edit.)... op. cit., pp. 80-98.

[17] Gołębiowski J., *Profilowanie kryminalne*, Warszawa 2008, p. 10.

on premises that can be appropriately substantiated. A criminal profile can be used also for determining the course of subsequent detection activities – not only for targeting perpetrators and verifying suspects, but also for preparing to procedural steps (interview – the content of the questions, search – a list of items etc.) and defining the course of further information acquisition.

Classification criterion: control methods

Case handling analysis – it is an assessment of actions taken and methods used thus far in a case in progress in order to establish the further course of action. This form is aimed at examining the actions taken and methods used in a case, and efficiency of information acquisition[18]. It applies to priority cases of serious crimes which are usually handled by dedicated investigation teams. In such cases, over several or more months, individual concepts of the investigators clash, various investigative methods bring different effects over time, the adopted versions either gain or lose importance in the course of their verification. Interactions within the investigators may lead to uncritical adoption of a specific direction by the group (one of the versions assumed) and persistent holding on to selected action methods, which in turn may lead to depleting the group's „arsenal". If that happens, cases come to a halt and even require a fresh look by someone from outside the investigation team who is not related to the case, and a criminal analyst is certainly such a person. Such analysis is rarely a standalone form, and its elements appear on the occasion of other analytical activities conducted. As already noted, the forms of operational analysis discussed above cannot be analogously distinguished in practice, as analytical activities do intermingle and complement each other in the course of criminal analysis, and they rarely remain in the original form defined in the classification.

Strategic analysis

Interpol experts note that the subject of strategic analysis includes long-term problems and objectives, research-based priorities and strategies for combating criminal activities and crime development forecasts[19]. In public security services, strategic analysis is applied to identifying and solving crime-related problems.

The scope of strategic analysis includes, most importantly:

- monitoring of general situation in the country,
- monitoring of individuals crime sectors,
- detecting new trends in crime,
- large criminal organisations,
- analysis of investigative methods,
- study of crime prevention,
- general crime statistics,
- evolution of efficiency of security-related activities,

[18] Analiza kryminalna (uaktualniona wersja 2.0.)..., op. cit., pp. 34-35.

[19] Analiza kryminalna (uaktualniona wersja 2.0.)..., op. cit., p. 16.

Strategic analyses regarding specific crime should take into account objective and coexisting information and data like e.g. demographic data, land development, geographic data – especially GIS linked[20], weather data, archived records, factual data, legal regulations, procedures etc. Some strategic analyses may require participation of or support from experts in various fields (including statisticians, lawyers, economists, psychologists) and mat have the form of comprehensive one-off or periodic reports. Strategic analyses serve the purpose of decision making regarding an entity's current matters and atypical or extraordinary situations, but they are also used in the context of long-term actions, plans and strategies of that entity.

Unlike operational criminal analysis, which is usually centred on a single case, strategic criminal analysis applies to the plural number of crimes, cases and phenomena. The period to which it applies is also clearly longer than in the case of operational analysis. Strategic analyses often present generalisations, summaries, trends, patterns and deviations therefrom, indicators of increase and decrease in crime rates, characteristics of a phenomenon etc. In practice, strategic analysis is conducted by criminal analysts much more rarely than operational analysis. In its final form, it often materialises as a report, statistical description, tables and geographic analysis.

Forms of strategic analysis

The respective forms of strategic analysis described below are more focused on the subject itself than actual methods of execution, thus leaving space for individual selection of working techniques which will be supported, on an ongoing basis, by new IT tools and scientific achievements.

Classification criterion: the crime

Crime analysis – it focuses on the type of crime subject to analysis (by category, type, specific Penal Code article and other criteria), more specifically its manifestation in a specific area and at a specific time. Such phenomenological approach will provide for identifying certain trends in crime, their unique characteristics, growth forecasts and operating plans and strategies of a given unit. Tables, charts and statistics presented in strategic analysis reports are more and more often complemented by findings of GIS[21] -based geospatial analyses (internal security agencies like the Police and national Revenue Administration use ArcGIS[22] software) where the use of maps is much broader than just the traditional indication of crime centres.

Classification criterion: the criminal

General profile analysis – it consists in establishing features characteristic of perpetrators of a specific type of crime which repeat or are similar in cases subject to comparison.

[20] Geographic Information System, GIS.

[21] GIS is a computer programme for digital maps.

[22] ArcGIS is made up of many elements with advanced functionalities for editing, cartographic analysis and presentation, and management of data.

General profile analysis can be widely used in, among others, situations that require communication with the general public (warning against perpetrators and their methods of operation e.g. a „grandson" scam), require quick reaction by State services (terrorist threats, kidnappings) or where selection of suspects or targeting of perpetrators must be accelerated (e.g. child abuse). The resulting personal characteristic (a profile of a perpetrator of a given type of crime) can be the basis for verification of actions taken so far and a point of reference for further actions – a unique control matrix.

General profile analysis uses, among others, analytical tools, spatial references (especially GIS-based), comparative analyses and tabulated summaries.

Classification criterion: control methods

Analysis of methods employed to solve cases – it is conducted to improve operating methods of persons in charge of conducting specific types of cases.

Despite the imposed (by regulations or orders from the superior) catalogue of actions relevant to the nature of the problem at hand, there are always certain disparities. They may relate to selection of operating methods, resources deployed, order of actions, special attention to specific issues etc. As a result, the degree of efficiency of those activities is different from unit to unit. The form of analysis in question is aimed at establishing which of the methods employed have had an actual impact on the positive result of the cases concerned, having regard to strengths and weaknesses of the actions. This form of analysis must take into account and compare factors that distort the objective picture of the reality – these may include e.g. the specific nature of a given area and crime that is characteristic of that area (trafficking in border areas), workload on officers performing the activities (the number of people in a given unit, vacancies, absences), what is the level of training of the officers, what equipment they have at their disposal to perform the activities (financial, communications, logistic resources...). Findings brought by analysis of methods employed to solve cases can be used in training, instructions, guidelines, circulars and specialist reports. They can also serve as an indicator of the need for organisational changes in a given unit.

The forms of operational and strategic analysis discussed above are undoubtedly versatile, which means they may be applied to combating any type of crime as well as to other activities undertaken by State services and agencies.

Respective forms of criminal analysis involve specific methods of operation which, when selected by an analyst, facilitate the achievement of the objectives of a given analysis.

It must be highlighted that those respective forms of criminal analysis are somehow too strict about the scope of analytical activities involved. This is probably due to the fact that they are more an effort to systematise the issue than present it in practical terms, as is especially seen in the forms of operational analysis, which intermingle and complement each other in practice. This is confirmed by experiences and findings from criminal operational analyses that have been conducted in Poland so far. However, it is advisable to familiarise oneself with respective forms of analysis employed in Poland and around the world due to their respective scopes of analytical activities. Also, these forms contribute to broadening the current definition of criminal analysis and its types. Individual forms of operational and

strategic analysis have been discussed with reference to the following three criteria – the crime, the criminal, control methods.

Type of analysis		Operational analysis	Strategic analysis
Criterion	Crime	Case analysis	Crime analysis
		Comparative analysis of cases	
	Criminal	Crime group analysis	General profile analysis
		Specific profile analysis	
	Control methods	Case handling analysis	Case methods analysis

Table 1: Forms of operational and strategic analysis (source: own research based on training materials of the Police Academy in Szczytno)

Role and sources of information in criminal analysis

Contemporary information management is becoming a domain of not only State services but businesses and private individuals as well. The growth in the number of sources of information and improvements of storage capabilities and the quality of processing make contemporary analysis a more effective and much faster process.

Criminal analysis, which is based on large volumes of data and information, must clearly keep up with the pace of general trends in modern day information analysis. Therefore, one must examine the process of information acquisition and methods of information assessment before it is logically processed and enters a „higher level" in the process of analysis and is translated into subsequent conclusions.

Criminal information analysis

In the informal sense, the terms „data" and „information" are often unknowingly equated although they are not synonyms. Data should be distinguished from information, for data is primary to information, which is a result of data processing. Therefore, using the term „information processing" may even bring negative connotations and be associated with manipulating information. Nevertheless, it is in fact possible to use the term „information processing" in the analytical process, which can be understood as a process of establishing knowledge by a given entity on the basis of information already acquired and substantially compiled to create a logical whole that will represent the foundations for decision-making processes. In the light of the above deliberations, one can clearly identify the distinction between the concepts of data, information and knowledge. Data most often has the form of unstructured facts gathered either by means of observation (content of conversations, number of meetings between specific individuals, number of deliveries and their nature etc.) or records on specific media (e.g. phone call data, web traffic data, IP numbers, data on financial transfers on bank accounts, e-mails etc.). The manner and source of generation of data give it a clearly objective character. To become information, data must be processed

by a human. Since the subsequent form of information depends on a subjective assessment and interpretation of data, different people can produce different information based on the same data.

Information is a product of processing of a series of data. If it is a result of a process of thought, it becomes a clear and intentional message from the author of information and, therefore, not only is it secondary to the data, but subjectively biased as well.

The term „criminal information" can be encountered in legislative acts (the Act on gathering, processing and providing criminal information[23]). Not getting into too much terminological detail, the legislator provides a broad definition of the term by stating that „criminal information – shall mean data, as defined in Article 13 Paragraph 1 [where the scope of criminal information is defined in detail – author's note], related to matters subject to operational and exploratory activities or initiated or completed criminal procedure, including procedures in cases of fiscal offences and other procedures or activities conducted under applicable Acts by entities specified in Articles 19 and 20 [these articles list entities authorised to receive and entities obliged to provide criminal information to the National Centre of Criminal Information – author's note] which is important from the perspective of the operational and exploratory activities of the criminal procedure"[24]. Gathered and subsequently stored, processed and provided by the Chief Commander of Police (as the obliged entity under the aforementioned Act), criminal information is in fact a collection of data and information which, in the course of further analysis, becomes the knowledge of a given unit. Information (also information a criminal analyst is interested in) should show certain characteristic features[25]:

- use of the information does not lead to its destruction, and it is not used during duplication and transport;
- it can be accumulated over a very long period of time;
- it is not fully divisible – a part of it may represent no information at all;
- a set of information is inexhaustible;
- it is a non-proprietary good – a replica does not differ from the original and has the same value as the original;
- information that is important to some entities may be useless for others;
- the value of information depends on when the information is used (what has some value today me be useless tomorrow).

These features are very universal and locate information (and its meaning) in every area of life, so they are an evaluative repertory also in the context of the State security.

Knowledge is defined as, among others, a resource of information on a specific field. It can be assumed that the sum of knowledge held by individuals that comprise a given organisation or entity represents „the entity's knowledge". However, volume of information does not always translate to the quality of knowledge, and the quality of information determines whether the

[23] The Act of 6 July 2001 on gathering, processing and providing criminal information; Journal of Laws 2010, No. 29, Item 153, as amended.

[24] Ibid.

[25] M. Olender-Skorek, K. B. Wydro, *Wartość Informacji*, Telekomunikacja i Techniki Informacyjne, tom nr 1- 2/2007, Warszawa 2007, p. 72.

knowledge is likely to be expanded. It often happens in the intelligence gathering process that the quality of information acquired leaves much to be desired. Of course, it expands the information resource of a given entity in terms of volume, but it does not contribute anything to the entity's knowledge.

Although a human is an extremely valuable (often the only) source of information, one cannot fail to notice other sources of information. Their number, availability and ease of gathering contribute to expanding the analytical potential. Always when criminal information analysis is mentioned, it is necessary to refer to resources from which the information was taken.

Sources of information in criminal analysis

Case files (material) delivered together with an order to conduct criminal analysis represent the main resource of data and information. However, also databases (internal and external), archives, registers and other sources (either closed or open) offer information resources that are of interest to a criminal analyst. Data and information are the starting point in the analyst's work, and a shortage of these makes every analysis poorer proportionally to the extent of that shortage. The Operational Information Centre is a rich database important to every Police officer seeking focused information, even more so for a criminal analyst. It is not, however, the sole database source that can be, and should be, used when conducting analyses (provided that each access to the database is substantiated). There are also other valuable sources of data and information. They are particularly important in the process of analysis, not only in terms of gathering and linking of information, but also in terms of verifying the adopted assumptions and hypotheses.

Depending on the needs and character of Police's criminal analyses (and also depending on the creativity of the criminal analyst), the criminal analysis process can be based on various databases; in the Police they are:

- Operational Information System (Polish: System Informacji Operacyjnej, SIO),
- National Police Information System (Polish: Krajowy System Informacyjny Policji, KSIP),
- Automated Fingerprint Identification System (AFIS),
- Police Register of Mass Events (Polish: Policyjny Rejestr Imprez Masowych, PRIM),
- [Road] Accident and Collision Register System (Polish: System Ewidencji Wypadków i Kolizji, SEWiK),
- „Weapons" Register,
- National Centre for Criminal Information (Polish: Krajowe Centrum Informacji Kryminalnych, KCIK),
- Central Register of Vehicles and Drivers (Polish: Centralna Ewidencja Pojazdów i Kierujących, CEPIK),
- Central Population Register (Polish: Centralna Ewidencja Ludności, CEL), including the Universal Electronic System for Registration of the Population (Polish: Powszechny Elektroniczny System Ewidencji Ludności, PESEL) and residence registration databases,
- Central Register of Issued and Invalidated Passports,
- the national set of registers, inventories and lists in matters regarding foreigners, named „System Pobyt",

- Visa Information System (VIS),
- National Criminal Record (Polish: Krajowy Rejestr Karny, KRK),
- Register of Convicts and Persons Held on Remand (Polish: Kartoteka Osób Skazanych i Tymczasowo Aresztowanych, KSiTA),
- Central Database of Detainees Noe.NET,
- Integrated Register System of the Border Guard,
- National Court Register (Polish: Krajowy Rejestr Sądowy, KRS),
- Business Activity Register (Polish: Ewidencja Działalności Gospodarczej, EDG),
- Register of Pledges (Polish: Rejestr Zastawów, RZ),
- New Land and Mortgage Register (Polish: Nowa Księga Wieczysta, NKW),
- National Official Business Register (Polish: Krajowy Rejestr Urzędowy Podmiotów Gospodarki Narodowej, REGON),
- broadly understood sources (some of which have already been mentioned) used during financial investigation and included in the Electronic System of Property Recovery (Polish: Elektroniczny System Odzyskiwania Mienia, ESOM),
- Database of Topographical Objects (Polish: Baza Danych Obiektów Topograficznych, BDOT10k)[26]
- international databases,
- other sources such as the government websites: GEOPORTAL and GEPORTAL 2, anonymous information, private opinions (specialists, experts), other open sources on the basis of which Open Source Intelligence is conducted[27].

Exploration of such potential of databases and sources of information (given the fact that it is not a closed catalogue) shows the variety of information and data that can be acquired, leading to rich knowledge that a criminal analyst can and should have. The multitude of information sources determines the quality of „criminal knowledge", so in consequence it is ineffective, and sometimes even unprofessional, for a criminal analyst to rely only on the material provided together with a request for criminal analysis. As for intelligence gathering activities, the management of information acquired by and then stored in respective databases requires its verification and appropriate utilisation. Therefore, information cannot exist only in a database, as its acquisition into the knowledge of a specific entity determines further dynamic and proactive approach, and this is where the analytical process is clearly visible. Concern for quality and quantity of information is becoming an immanent feature of intelligence operations, including the analytical process. However, the volume and quality of information itself has always been related to the assessment of both information and

[26] The Georeference Database of Topographical Objects (Polish: Georefernycjna Baza Danych Obiektów Topograficznych, BGDOT), created by the Head Office of Geodesy and Cartography, will provide topographical and geographic data gathered by Poland's Geodesic and Cartographic Service to public institutions and business entities that use geoinformation systems in their operations and in order to support decision making processes with the use of classic GIS IT tools, available also on www.geoportal.gov.pl; source: the website of the Head Office of Geodesy and Cartography http://www.gugik.gov.pl/projekty/gbdot, as of 14 January 2014.

[27] More on Open Source Intelligence, OSINT, in K. Radwaniak, P. J. Wrzosek, Biały wywiad w Policji – pozyskiwanie i analiza informacji ze źródeł otwartych, [in:] J. Konieczny (edit.), Analiza informacji..., op. cit., pp. 109-150.

its source. Only a uniform method of assessment of information and its source can ensure a transparent manner of gathering and processing of already evaluated information, thus leading to making accurate, premeditated and safe decisions.

System of assessment of information and its sources (4x4)

Gathering information, every State service makes efforts to verify and use it. However, this requires time and the circumstances often make it necessary to evaluate information on an ad hoc basis. Although quality of every piece of information is initially assessed the author of the document, every person who can, in its professional capacity, use that document also assesses its quality and reliability. The information assessment system, in service with Polish services for many years (both under the Peoples' Republic of Poland and the modern day Republic of Poland), was far from ideal and the manner of knowledge distribution was limited mainly to assigning and transferring traditional documentation to a selected unit. To deepen information provided by another officer (often from a different unit), especially in the context of assessing its reliability, the recipient had to contact that officer, either directly or indirectly, which was not always possible. Later on, as the IT technology developed, some data was sent to database systems, but a lot of valuable knowledge still ended up in file cabinets or even in officers' memory, as it had never been put to paper. As a result, some information was somehow „privatised" or restricted to, most often, local use. In such situation, it became necessary to change the system of information handling, especially in the context of its assessment and further use.

In order to implement a uniform method of processing and interpreting information as well as assessing information and its sources, the „4x4" information assessment system[28] was adopted by the Polish Police and other internal security forces. The name suggests a product of respective reliability codes – there are four codes assigned to the source and four codes assigned to information coming from the source. This system has brought an individualised manner of assessment of information on a piece-by-piece basis.

The idea behind assigning codes to the source and, separately, the information is to ensure effective assessment of those two elements while maintaining uniformity of the system across the entire police force (and subsequently other forces). It produces a comprehensively assessed information report which can be used at any time (provided that applicable internal regulations have been met). The decision-making process is also accelerated thanks to the unified rules of interpretation of coded reports, as the 4x4 codes are both assigned and decoded according to unified guidelines.

Although descriptions of respective source and information codes have undergone minor changes over the last decade, the sense of the codes has remained unaffected. At present, the following assessment codes are used:

– source codes

1) code „A" – no doubt about the reliability of the source;

[28] The system is used also by Europol and a number of EU Member States.

2) code „B" – source from whom information received has in most instances proved to be reliable;
3) code „C" – source from whom information received has in most instances proved to be unreliable;
4) code „X" – information comes from a new source, whose reliability is unknown because the source has not been or cannot be verified.

– information codes
1) code „1" – information is assessed as true by the officer;
2) code „2" – facts referred to in the information are known personally to the source;
3) code „3" – facts referred to in the information are not known personally to the source but are corroborated by other sources;
4) code „4" – facts referred to in the information are not known personally to the source and cannot be corroborated.

Sources marked as A or B are regarded as reliable, however they may acquire information directly or indirectly. In addition, information may or may not be possible to corroborate at a given moment (even partially). In this light, only reports marked as A1, A2, B1, B2 count as reliable information, whereas all other codes (A3, A4, B3, B4, C1-4, X1-4) count as unreliable, although it does not mean that the information is untrue. They are part of the information resource of the organisation (here – the Police), but they require further actions to be reliably verified.

The system of assessment and protection of information and its sources is a comprehensive solution that provides significant support to the foundations of criminal intelligence. It is also a versatile solution which can be successfully deployed by entities outside the Police force which are authorised to acquire and gather information. Appropriately assessed and safely stored information becomes the starting point for its analysis. The role of criminal analysis is efficient use of information gathered in database resources by means of finding relations and connecting them (in a given case) in a logical whole that gives grounds for further conclusions.

The table below presents information reliability assessment (based on informational materials of the Criminal Intelligence Office of the National Police Headquarters, BWK KGP)

Techniques and tools used in the process of criminal analysis

Techniques used in criminal analysis

Criminal analysis techniques presented in this subsection have been unified in order to simplify their application and interpretation. To assess their universal nature and ability to be deployed by many entities and in many fields of operation, one must first review characteristics of those techniques and principles of their visualisation.

Visualisation of information

Analytical techniques boil down to visualisation of information contained in the material at hand which has been selected by the analyst from „the information chaos" and subsequently presented according to principles of a given technique. Most information and data in case files (also on other storage media) is unstructured. Both systematisation of the material and

SOURCE ASSESSMENT CODE Source reliability assessment		INFORMATION ASSESSMENT CODE Relation of source to information			
		Information is true without any doubt	Information is known personally to the source	Information is not known personally to the source but corroborated by other information already recorded	Information is not known personally to the source and cannot be corroborated
		1	2	3	4
There is no doubt of the authenticity, reliability and competence of the source, or information is supplied by a source who, in the past, has proved to be reliable in all instances	A	A1 Officer of the Police, court, prosecutor's office, police working methods, procedurally proven results	A2 Officer of the Police, court, prosecutor's office, police working methods, procedurally proven results	A3 Officer of the Police, court, prosecutor's office, police working methods, procedurally proven results	A4 Officer of the Police, court, prosecutor's office, police working methods, procedurally proven results
Information is supplied By a source who has in most instances proved to be reliable	B	B1 Other state administration officers Databases, including ZSIP, KSIP, OPIS, TBD WEP, Temida, extracts from land and mortgage registers etc., Informant with long service record who has always proved to be reliable.	B2 Other state administration officers Databases, including ZSIP, KSIP, OPIS, TBD WEP, Temida, extracts from land and mortgage registers etc., Informant with long service record who has always proved to be reliable.	B3 Other state administration officers Databases, including ZSIP, KSIP, OPIS, TBD WEP, Temida, extracts from land and mortgage registers etc., Informant with long service record who has always proved to be reliable.	B4 Other state administration officers Databases, including ZSIP, KSIP, OPIS, TBD WEP, Temida, extracts from land and mortgage registers etc., Informant with long service record who has always proved to be reliable.
Information is supplied By a source who has in most instances Proved to be Unreliable.	C	C1 Most information from informants which require additional verification	C2 Most information from informants which require additional verification	C3 Most information from informants which require additional verification	C4 Most information from informants which require additional verification
Information is supplied By a new, unassessed source Whose authenticity, Reliability and Competences are unknown, Or information is supplied by A new, unassessed source Whose Authenticity, reliability And competences cannot be confirmed.	X	X1 Newly acquired sources (informants) whose reliability is yet unknown, a witness, unidentified and highly unreliable sources who supply information only once or who, when supplying information, clearly and intentionally „juggle" with their knowledge – all media – all newspapers, radio stations, TV stations and the internet,	X2 Newly acquired sources (informants) whose reliability is yet unknown, a witness, unidentified and highly unreliable sources who supply information only once or who, when supplying information, clearly and intentionally „juggle" with their knowledge – all media – all newspapers, radio stations, TV stations and the internet	X3 Newly acquired sources (informants) whose reliability is yet unknown, a witness, unidentified and highly unreliable sources who supply information only once or who, when supplying information, clearly and intentionally „juggle" with their knowledge – all media – all newspapers, radio stations, TV stations and the internet	X4 Newly acquired sources (informants) whose reliability is yet unknown, a witness, unidentified and highly unreliable sources who supply information only once or who, when supplying information, clearly and intentionally „juggle" with their knowledge – all media – all newspapers, radio stations, TV stations and the internet

Table 2: Information reliability assessment (source: own research based on informational materials of the Criminal Intelligence Office of the National Police Headquarters, BWK KGP)

selection of information for the purpose of visualisation are a result of the analyst's original design. Diagrams that reflect information are not a fresh concept, as they have been in use in practically every field of science. Diagrams give grounds for fast perception of complex issues and lead to faster and more substantive conclusions.

Visualisation of information according to a selected analytical technique plays two roles in criminal analysis. Firstly – it is an element of the analyst's working arsenal. Building a „working" diagram, an analyst processes large volumes of information in it and is thus able to more easily understand, assess and find connections. In practice, such „working" diagrams are very complicated, but since the analyst creates them himself or herself and devotes a lot of attention to them, he or she is able to „master" the multitude of information on analytical objects and connections between them. Visualisation is also a product which serves the analyst to establish contact with the recipient of the analysis. It is a bridge between text information and its graphic representation. By means of a working diagram, the analyst subsequently creates the final diagram by selecting the appropriate layout (e.g. hierarchical, centred), removing redundant line intersections and making simplifications (by resigning from not important elements which can be replaced with a brief comment or a key). The effects of the analysis will be achieved if the final diagram/diagrams is/are a clear guide to the analyst's report, where, on the one hand, it is a source of information (sometimes even inspiration) itself and, on the other, facilitates comprehension of further content of the report that refers to the diagram.

Processing text information into an image is, contrary to what one may presume, a simple action that is carried out methodically and according to certain general rules related to the objective and layout of the diagram as well as its clarity and currency.

Objective of the diagram

Since every diagram serves a certain purpose, its objective is selected in parallel with selection of an intended analytical technique. The objective of a diagram is achieved by projecting information that comprises the final „picture". The objective is usually physically present either in the title or description of the diagram e.g. „A diagram of capital connections of company X. The aforementioned title includes information on the analytical technique employed (a diagram of connections) and the purpose of the technique (presenting capital connections of a selected entity).

Layout of the diagram

Designing a diagram is related to selecting an appropriate layout of presentation – i.e. graphic arrangement of individual elements. Although the spatial arrangement of a diagram is largely depended of the selected analytical technique, it is the analyst who decides about the perspective. If a diagram is to show the hierarchy of a specific organisation, then it is advisable to present the structure starting from superior objects and going on to subordinated objects (top-down approach). In this case, the analyst can distinguish respective levels of objects that have equal ranks within the organisation. On the other hand, the centred layout shows the key object (objects) in the centre with branch lines (connections with other objects). This layout

is also referred to as „a peacock tail" (after the command in menu of analytical software). Finally, chronological diagrams can show proportional time intervals between individual events (but then there is a risk of extending the diagram with „empty" periods with no event-related components) or be clustered without time proportions so that individual event frames could be squeezed into the smallest space possible while maintaining their order (chronology).

Clarity of the diagram

How easy it is to interpret a diagram will depend on its clarity. The fewer objects there are in a diagram, the clearer it is. Analysts should avoid, if possible, intersections or bends in the lines that connect objects, contact between objects, overlapping descriptions, too many colours or unnecessary „ornaments". Clarity of a diagram is related to its perception by persons for whom it was created, and since, as already mentioned, it is „a guide" to information, its clarity will affect the overall reception of the analysis. In most cases, analysts work on the so-called „working diagram" (which includes most of the information shown in the graph), which can later be transformed into a clearer form to be presented to the recipients of the criminal analysis. Left on the final diagram are the most important analytical objects and connections accompanied by a description (every diagram must have a comment, a reference to the material).

Currency

Every diagram is created on the basis of specific information. The information, contained on numbered case file sheets (or other storage media), present the situation as of a specific day. A diagram is current as of a specific moment, i.e. the moment at which the analyst works on specific information acquired at specific time. Every diagram must be marked with the date of its creation (sometimes even the time), which makes it clear later on why it does not contain e.g. information acquired after its creation but, at the same time, provides for maintaining the chronology. The above guidelines are universal and apply to all methods of visualisation of information, while referring mainly to the roles that such visualisation should play (as noted at the beginning of this subsection).

The analytical techniques presented below are reflected in practice, especially in relation to criminal operational analysis. This is so because of the differences, discussed earlier, between various forms of criminal analysis (strategic analysis may be based on a different methodology, often borrowed, e.g. CRISP-DM125).

The matrix – an element of working with a diagram

Before proceeding to reflecting information on a graph (mainly in a diagram of connections), one can use the aid of the matrix (Figure 2). The purpose of the matrix is to structure and list objects and mark relations that occur between them. It has an ancillary role in creating a diagram and provides for its subsequent control in terms of consistency between data in the matrix and on the graph.

Connections between objects are plotted on the matrix with the use of appropriate coding which corresponds to the „4x4" system of information/source assessment. Matrix coding

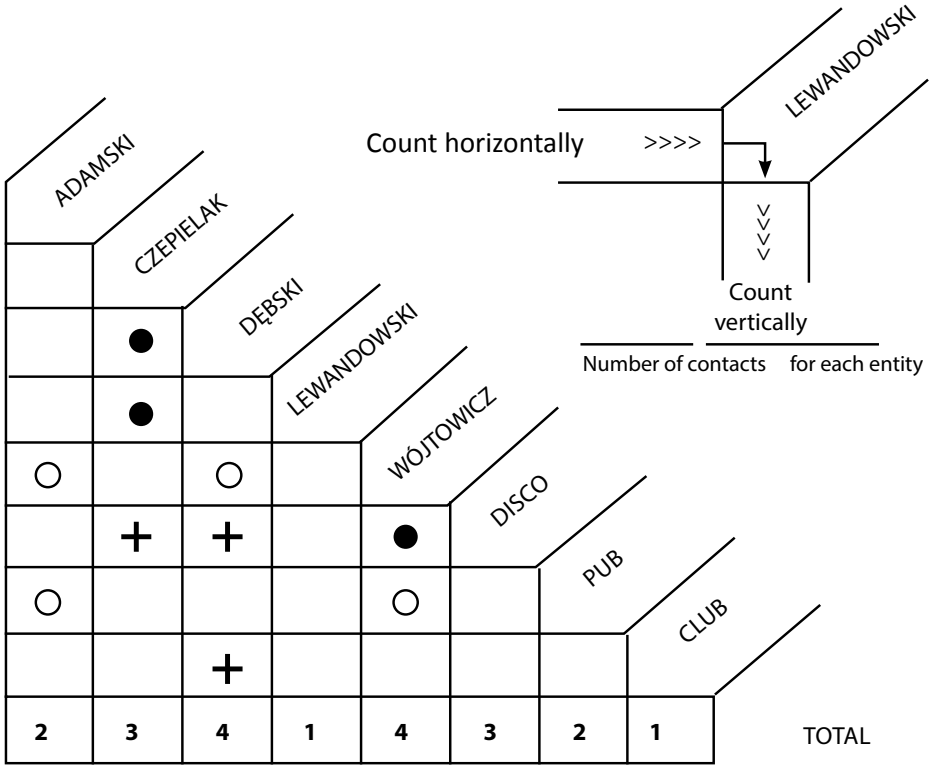


Figure 2. A completed matrix of connections (Source: *Wybrane zagadnienia analizy kryminalnej,* W. Iganczak, Szczytno 2005)

is aimed at providing correct presentation of relations between respective analytical objects and the nature of those relations (e.g. confirmed – unconfirmed information).

A carefully completed matrix ensures that all connections of interest that are contained in the material are maintained (with due regard to „function holders", who are marked with „+"), provides for establishing the number of objects with the greatest number of connections and is the starting point for creating a diagram of connections (especially a working diagram). The matrix can also be used for preparing a statistical summary of contacts between one person and another person or object, establishing who and when participated in a specific event, was present at a specific place etc.

Diagrams of connections

A diagram of connections is a graphic projection of relations between persons, organisations or items present in a case. Interconnections can be seen in any personal configurations as well as connections between persons and organisations or items, and other non-personal relations. Diagram of connections is an analytical technique which can be used in any case, provided it is required. Obvious and simple relation configurations (e.g. between only a few objects) do not require visualisation, but a decision to resign from visualisation should be made on a case-by-case basis.

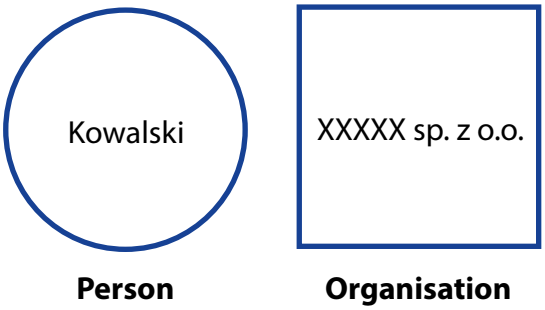


Figure 3. Symbols used in a diagram of connections (source: own research)

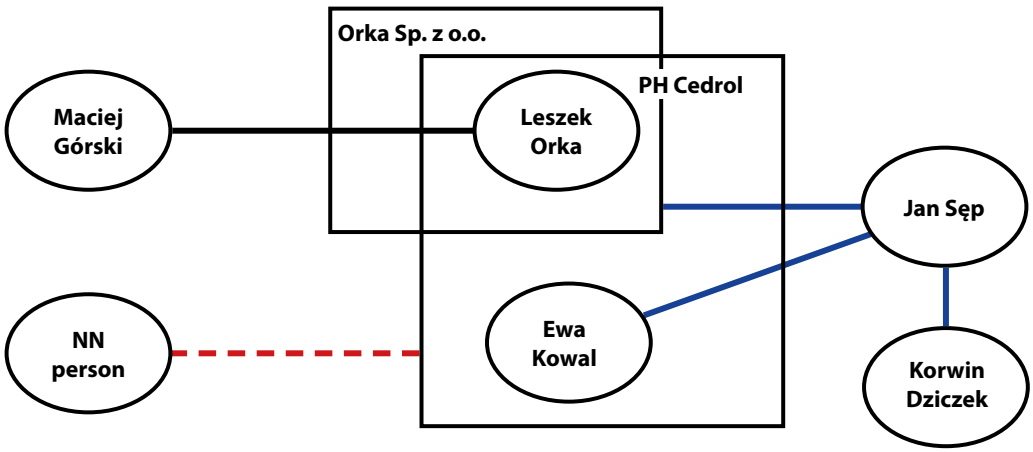


Figure 4. Diagram of connections between persons and organisations (source: based on training materials of the Police Academy.)

Criminal analysis has uniform methods of visualisation of information by means of simple symbols. Before computers entered into mass use and dedicated computer applications arrived, analysts would use two geometrical figures to represent specific analytical objects. Circle was for persons and rectangle for organisations (Figure 3), broadly understood as all analytical objects other than persons (crime organisations, addresses, locations, economic entities etc.).

A criminal analyst can present confirmed and unconfirmed information with, respectively, a continuous or dashed line linking the edges of objects (as objects connected according to the case material). Persons who are in charge of or have actual influence on the functioning of a specific organisation (e.g. a landlord and a rented flat, a company and its owner, director, shareholder) are represented by oval shapes inside a rectangle (Figure 4).

As the IT technology progressed, computer solutions entered into the domain of law enforcement agencies and led to adapting the functionalities of analytical applications to traditional principles of visualisation. As a result, the ability to visualise all information became increasingly more advanced in terms of graphics and intuitive in terms of message.

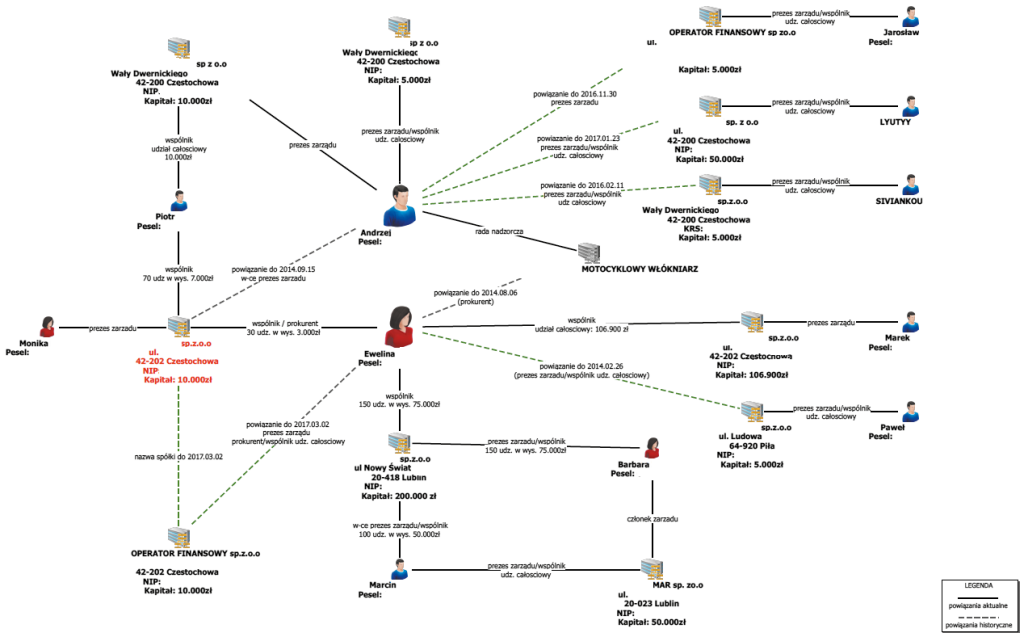


Figure 5. Diagram of connections created in i2 Analyst's Notebook (source: Own research)

Diagrams of connections are of significant importance in, among others, presenting connections within organised crime groups, capital connections between economic entities and visualising social networks. They assist in noticing intermediary objects, nodes and points of key importance in the flow of information etc. (Figure 5). In the case of complicated and complex networks, analysts can present a general picture of connections with lines reflecting interconnections between key objects, and then „unfold" the baseline picture into several others presenting selected fragments in greater detail in separate diagrams (top-down). This provides for showing a general picture of all key connections and then moving on to smaller branches of the relationship network. This approach to presenting connections can be reversed to the „bottom-up" approach. As always, it is dependent of the analyst's design and the recipient of the analyst's report (whether oral or written).

Diagrams of flows of goods and services

The purpose of diagrams of flow is to show the actual routes along which goods (tangible and intangible) are moved from one object to another (e.g. person to person or location to location). They are not much different from diagrams of connections (analytical objects are also represented by circles and rectangles), with arrows put in place of connections to show the direction of flow of given goods (Figure 6).

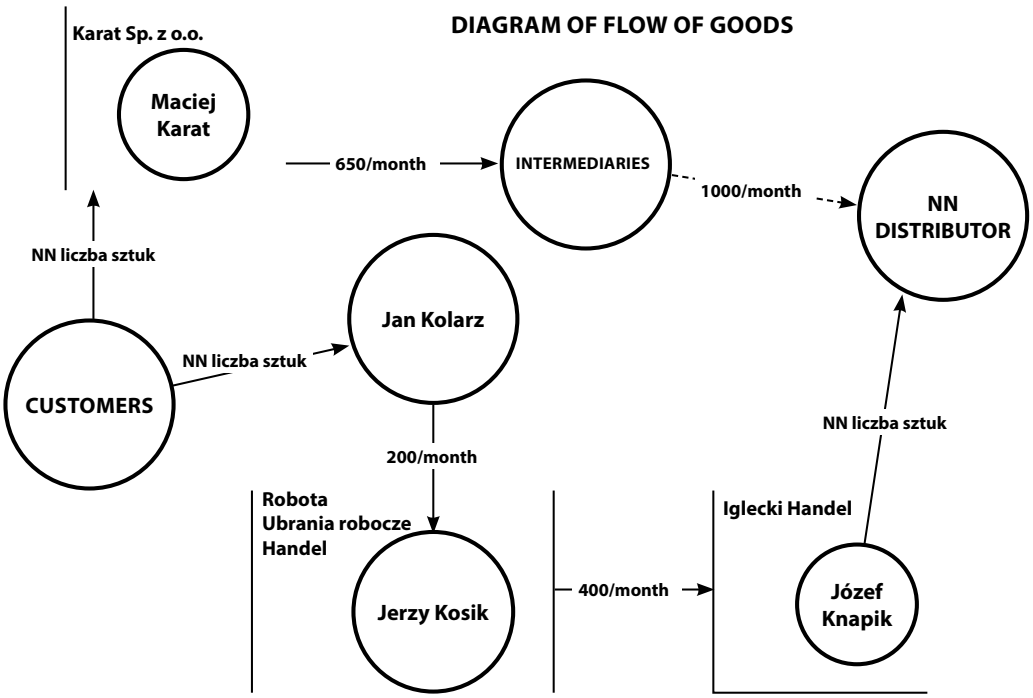


Figure 6. Diagram of flow of goods using the „traditional" symbols (source: *Wybrane zagadnienia analizy kryminalnej*, W. Igan-

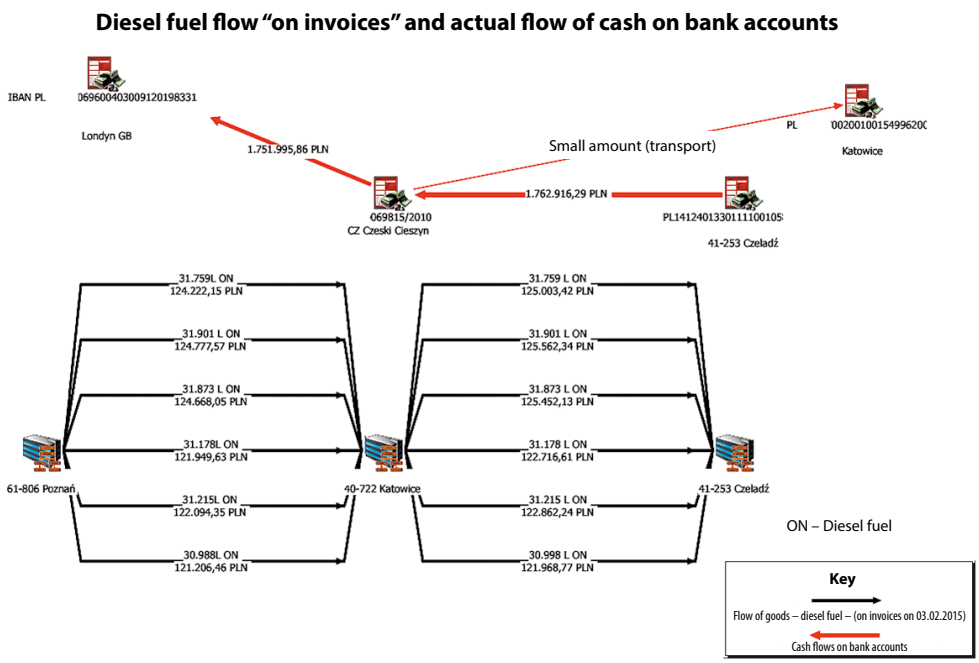


Figure 7. Diagram of flow created in Analyst's Notebook (source: Own research (identification details of the entities and accounts were removed for the purpose of this paper)

They provide for e.g. identifying the weakest link in the flow of goods or taking stock of the flow if even scarce or estimate information on the volumes moved is available (unit of weight or measurements).

Diagrams of flow of goods and services are very useful when it is required to analyse data obtained from different sources (often containing thousands of records e.g. call billings, bank transactions) which provide indications of the direction of transfer of given goods. Then it is necessary to present the data in a manner that can be understood by the principal and in accordance with the principal's expectations. Apart from visualisation of analytical objects, analysts use also analytical computer tools (e.g. mathematical computations, reference to dates, weekdays etc.).

Diagrams of event chronology

Chronological diagrams, showing systems of events, their chronology and interactions provide to viewing an issue from a time perspective. In order to create a chronological diagram based on a specific case, issue, fragment of reality, one must first isolate a set of information that comprises a series of individual smaller occurrences, which will in turn translate into a full picture of an event (phenomenon). Such information is presented in the form of diagrams of events and chronological analysis of events.

Diagrams of events are shown in the form of chronologically arranged descriptions of individual events (with a contour line around the text) connected with arrows (from left to right). They provide for simple and relatively fast presentation of key time-related issues. Time is described in boxes and/or on a timeline located above the diagram (Figure 8).

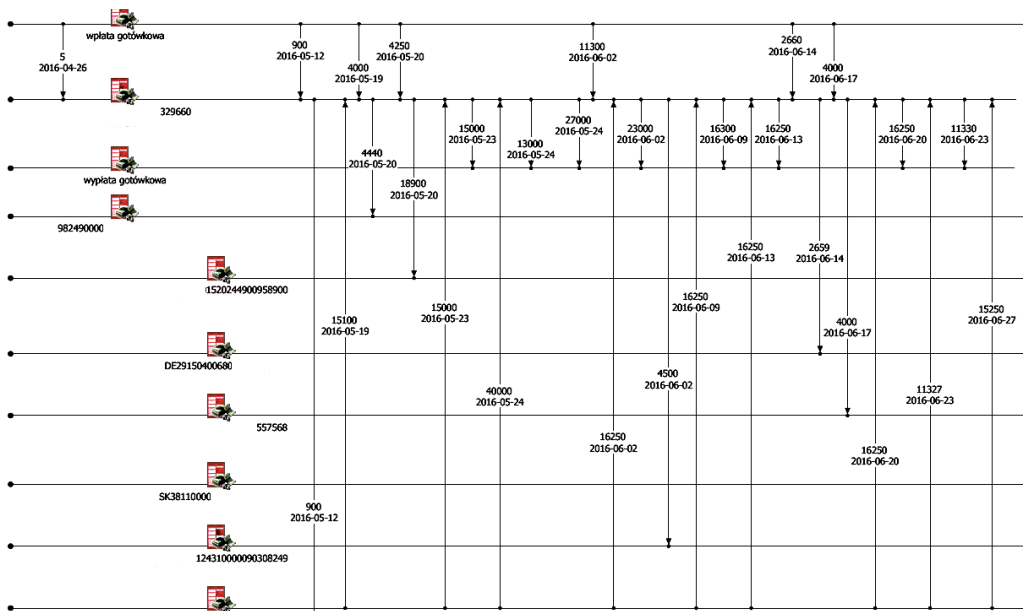


Figure 8. Chronological diagram of financial flows (source: own research – identification details were removed for the purpose of this paper)

Diagrams referred to as an event chronology analysis are more complex in terms of graphic. In addition to boxes with analogous events as in diagrams of events, they also use so-called theme lines to mark, most often, persons, companies, phone calls, bank accounts, actions (also crimes) and others (Figure 9).

Added to the theme line running along the timeline are event boxes related to that line. Some events are connected by two or more theme lines. Phone calls and bank transfers made are visualised in the form of arrows (vertical) that connect respective theme lines and show the direction of a call or financial Operation. Theme lines require following the events assigned to them individually or converging on other lines if the event relates to a greater number of themes. They provide for conducting multifaceted analyses of temporal relations between data and information, cause-and-effect relations and for identifying gaps in the material or the so-called „collisions of events" i.e. mutually exclusive information. These diagrams are excellent for making and verifying hypotheses.

For example, there are four witnesses in case „X" who give their accounts of events that happened over two specific days. Each of them gives their version of the events as they remember it or want to be seen as such. Therefore, we have four lines on which individual event components are put, but their descriptions or locations in time are different. A diagram created in this manner will provide for detecting all differences, analysing inconsistencies and preparing for further activities (e.g. preparing a plan of confrontation of the witnesses) or getting to other sources of information that will make it possible to verify the current information (e.g. CCTV recordings, other witnesses).

Events chronology analysis relies also on analyst software which can generate diagrams automatically to compare various information (e.g. invoice data vs. transport data, data from banking systems vs. documentation of a company).

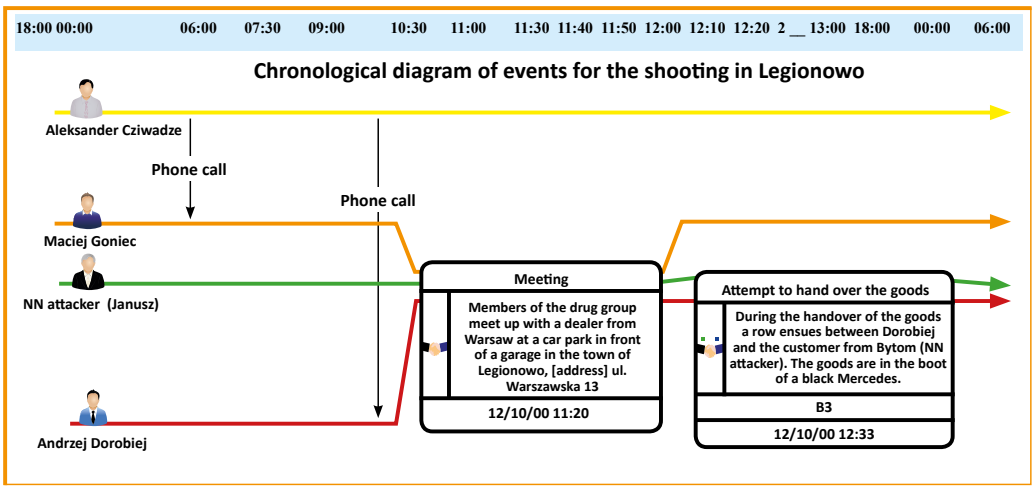


Figure 9. Diagram of events chronology showing theme lines and event boxes (source: M. Hausman, *Wykorzystanie analizy kryminalnej w działaniach podmiotów realizujących zadania na rzecz bezpieczeństwa Rzeczypospolitej Polskiej*, Wyższa Szkoła Policji w Szczytnie, Szczytno 2014)

Diagrams of activity

The purpose of diagrams of activity is to show the mechanism of a criminal activity by means of a universal template which can be applied to every type of a given crime. By answering the question „how was it done?", the diagram is meant to be forward-looking and answer the modified question „how can it be done?" Diagrams of activity are created in a similar manner as diagrams of events. The principal difference is that diagrams of events concern a specific case and its individual course with regard to the time of each minor event component, whereas diagrams of activity show a set of future actions without putting them on a specific timeline.

Studying actions taken as part of a given crime leads to putting them on lines of independent and interdependent activities. Some activities determine next activities and some can be done without affecting other activities (e.g. setting up a company website does not require paying VAT, so these two activities can happen independently). As a result, activity models are created that can be useful in terms of a phenomenological approach to criminal groups, but also e.g. in reference to antiterterrorist operations or security of IT systems (also in reference to any other issues where a set of repetitive actions can be observed).

Comparative analysis

As already mentioned in the above discussion of various forms of operational analysis, comparative analysis of crimes is aimed at establishing whether specific crimes (behaviours) could have been committed by the same perpetrator or group.

DIAGRAM OF ACTIVITY INDICATING THE METHODS AND ESCAPE IN THE EVENT OF A SERIES OF BANK ROBBERIES

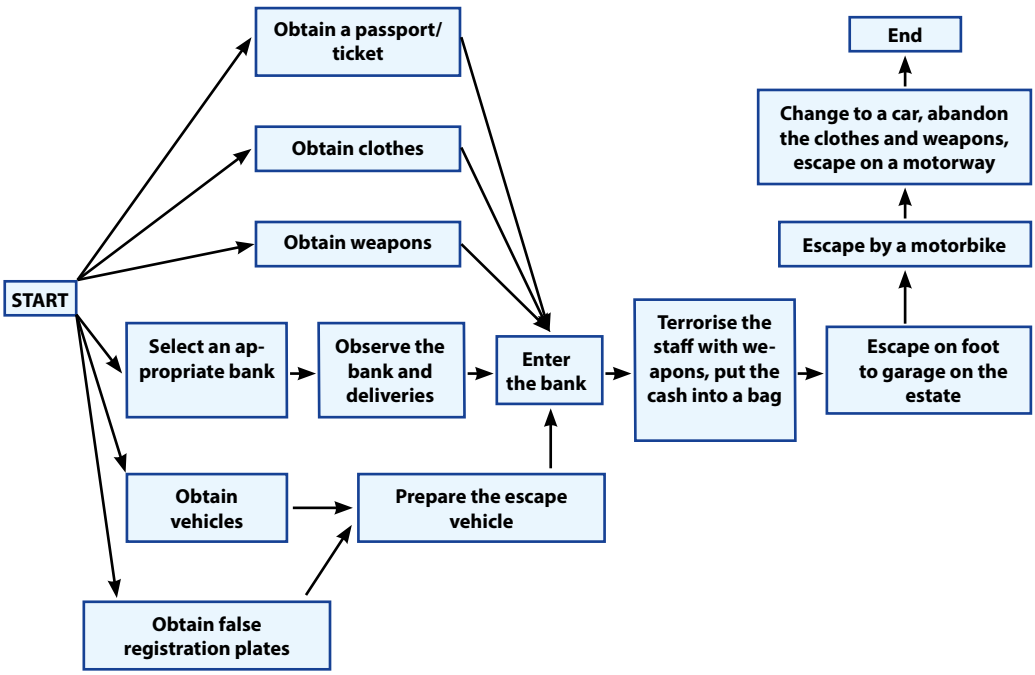


Figure 10. Diagram of activity (source: own research based on a training material)

Analytical activities consist in establishing criteria according to which individual cases are compared. Appropriate selection of the criteria is very important, as not all criteria can be found in each case. Criteria that are unclear and raise doubts about interpretation should be avoided because they should, when combined, show convergences and divergences between individual features and thus assist in assessing or excluding the likelihood that a crime is serial. Technically, such analysis should be conducted with the use of a table where selected comparison criteria are on one side and cases selected for comparison on the other (Table 3).

Such tabulated comparative analysis will ultimately lead to detecting the key convergent features of the cases compared, as well as differentiating features. It will therefore involve a quantitative (convergences) analysis and, more importantly, qualitative analysis, both of which will affect the criminal analyst's final assessment of the likelihood that the crime analyses is serial. Of course, such analysis does not boil down only to comparing characteristic features of crimes in a table, as a thorough examination of case files and materials is conducted both before and after it.

Each of the aforementioned analytical techniques is applied mainly in the course of criminal operational analysis. Thanks to their universal nature, which provides for examining information from various types of sources, they can be employed by a number of entities which make short-term or strategic decisions based on information resources.

Each of the aforementioned analytical techniques is applied mainly in the course of criminal operational analysis. Thanks to their universal nature, which makes it possible to use them with various sources of information, they can be employed by a number of entities which make short-term or strategic decisions based on information resources.

Tools used in criminal analysis

In the present age of a fully computerised society, we leave a lot of electronic traces behind us when we use our computers, tablets and smartphones. All these pieces of information that we leave when shopping online, visiting social media and using messengers can be analysed and linked in one coherent and clear whole. However, it cannot be done with classic methods, which is why currently every criminal analyst relies on analytical software e.g. Analyst's Notebook, iBase, Link and ArcGIS.

Analyst's Notebook

Analyst's Notebook works in conjunction with iBase software. The programme is used for graphic presentation of objects and connections between them in the form of charts and for processing of gathered information. Depending on the type of data, objects are shown on a chart as icons and other symbols like theme lines, event boxes, rectangles, circles, text blocks, OLE objects. Relations between objects are presented in the form of continuous or dashed lines or arrows which link the objects. In Analyst's Notebook, elements of a diagram are described with labels, identifiers, descriptions and classifications, time, information sheets, attributes and comments. The user can create or modify objects, attributes and types of connections and create own diagram templates. The user can either create diagrams directly or import data from other sources of information like iBase, txt files and Excel calculation sheets based

Bank burglary			
Name of bank	Bank Ochrony Środowiska w Sxxxxx	Bank Spółdzielczy w D...xxx	Bank Gosp. Region. Jxxxxx..
Address	Sxxxxxx, ul. Biała 2	D...xxx, ul. XXX-lecia 16	Jxxxxx.., ul. Pola 5
Date	2012-09-25/26	2012-10-08/09	2012-11-15/16
Day of week	Tuesday / Wednesday	Monday / Tuesday	Thursday / Friday
Burglary start time	23:40	02:20	00:40
Burglary end time	01:30	03:10	01:50
Time of discovery	06:20	05:25	02:20
Alarm system			
System specifications	communications with the centre: GSM, motion detectors, glass break detectors, CCTV cameras, external and internal acoustic signalling, alert to the monitoring centre	communications with the centre: TPSA and GSM, motion detectors, glass break detectors, vault and ATM opening detectors, visual and acoustic alarm on the building and alert to the monitoring centre	communications with the centre: TPSA and GSM, motion detectors, glass break detectors, vault and ATM opening detectors, internal and external visual and acoustic alarm, and alert to the monitoring centre
Fitter	Morski-Systemy Alarmowe	ASsecurity	ASsecurity
Monitoring	Mobilsafe – security agency	Tarnowski – site protection	Mobilsafe – security agency
Location			
Type of locality	town, seat of municipality	town, seat of municipality	miasto powiatowe
Positioning	at a side street, 200 m of a main transport route (E-8)	at a main road (municipal road)	at a main street (provincial road)
Characteristics of the premises	premises is fenced; used only by the bank; a new bank building is being built on the premises; a detached one-storey building with an attic,	premises is not fenced and has an illuminated car park; thick shrubs along the street, up to 1.40 m in height, obscure half of the building except for the entrance; the building is used only by the bank	the bank is situated in a strip of commercial buildings; the premises is not fenced and offers a direct access to the entrance
Building type	a detached one-storey building, in use	a detached one-storey building, in use	Part of terraced development, one storey
Modus operandi			
Defeating the alarm system	jamming the GSM signal and cutting off the TPSA line (in the telecommunication well, unnecessary from the technical point of view), destroying CCTV cameras and alarm siren, seizing the computer with CCTV footage	jamming the GSM signal, destroying the acoustic signal device and external CCTV camera, destroying the alarm panel inside the building	jamming the GSM signal, destroying the visual and acoustic signal device, CCTV camera and alarm sirens, seizing of the computer with the CCTV footage
Method of entry	tearing the window bars out and defeating the lock, cutting the ATM wall open (inside)	tearing the window bars out and defeating the lock, cutting the ATM wall open inside the building	tearing off and removing the padlocks from the window bar at the back of the building, forcing the window open, cutting the ATM wall (inside), blocking the access route to the back of the bank with a rubbish container
Tools used	crowbar, hammer, disc grinder	crowbar, disc grinder, power drill	crowbar, hammer, disc grinder

Table 3. Comparative table – bank burglaries (source: own research, based on Police Academy training materials)

on own predefined import templates. Using an intuitive dialogue window, an analyst defines the method of interpretation of input information (division into records and record fields) and its visualisation in the form of objects, connections, attributes and information sheets. An analyst defines the manner in which object attributes (like the identifier and label) are filled and linked by selecting appropriate record fields. The software provides for creating various layouts depending on the currently used analytical method. It allows the user to present the structure of connections between objects or emphasise chronology of events. It also provides for creating mixed diagrams which combine features of the types of diagrams mentioned above. The manner of presentation of objects in a diagram allows the user to automatically toggle between individual layouts (hierarchical, minimum intersections, pie chart, peacock tail, proportional, ranked, grouped).

Analyst's Notebook offers many analytical functionalities. It allows the user to:

- conduct graphical search for single and connected elements, enabling search by a type of object, text criteria, number criteria, date criteria, attributes, mixed criteria;
- conduct a text-based search for objects, connections as well as objects and connection combined, enabling inclusion of object components, as well as advanced search by multi-meaning symbols or regular phrases;
- search for indirect connections between remote objects taking account of the time and direction of connections and values of object and connection attributes;
- search for clusters in a group of connected objects taking account of the strength of ties and importance of connections;
- search for similar objects based on predefined criteria of compared texts;
- place diagram elements in the background and hide selected objects;
- generate reports based on diagram components;
- merge objects.

iBase

iBase database software is an efficient and user-friendly tool that supports the process of analysis. It allows the user to gather information on objects and relations between them. The software is used for supporting specific investigations where it serves as an integrated analytical base which unifies the standard of information that comes from multiple sources. iBase offers numerous functionalities, the most important of which include:

- easy creation of new and modification of existing database models to reflect the unique character of a specific case (characteristic types of objects and connections);
- fast entry of information on groups of connected objects;
- flexibility of import of information from external sources;
- a wide array of specialist analytical functions;
- full compatibility with Analyst's Notebook;
- easy management;
- scalability.

Work with iBase allows the user to create and adapt the database configuration via a clear graphic user interface. The existing database configuration can be modified during investigative

or operational or exploratory activities (e.g. by adding new types of objects and connections, adding new fields to the existing ones). It is particularly useful when an investigation is going in a new and unexpected direction.

iBase provides for fast entry of information by means of the dedicated data forms which are formulated at the stage of preparing the database design. The form can be adapted not only for entering new objects, but also for analysing their connections with objects already in the database.

The database software allows the user to import data from various types of sources like text files, OLE DB or XML files. Input data is processed into objects and connections specific for a given database structure, which ensures a uniform standard of information coming from different sources. Analysts import data by means of import templates, i.e. settings defined by the analyst, which determine the manner of interpretation of the input data and the manner of its processing to objects and connections.

iBase was designed for analysts. It offers several user-friendly analytical functions, the most important of which are:

- queries,
- operations on data sets,
- search for similar records,
- ranked similarity models,
- text search, generation of reports.

The software ensures full integration with Analyst's Notebook. In practice, analytical functions of Analyst's Notebook can be used in relation to information in iBase. Importantly, a significant portion of iBase functions is available from the Analyst's Notebook level. Selection of the working environment is entirely the analyst's decision. Compatibility with Analyst's Notebook expands the analytical potential by allowing analysts to:

- quickly reveal interconnections hidden within the data on Analyst's Notebook charts;
- identify critical connections among many different connections;;
- search, view and edit iBase records from the Analyst's Notebook level;
- create iBase object and connection records from the Analyst's Notebook level;
- expand objects on charts to view connections and connected objects without the need to go back into the database;
- view iBase records (e.g. events) on timelines with chronology.

Administration of iBase databases is easy. The software has two modules: a user module – called iBase User, and a designer module – called iBase Designer.

The administrator/designer module provides for designing database structure by defining types and properties of objects and connections, and configuring security. The user module provides for using databases by creating or editing records and analysing the data. The roles of designers/administrators include:

- designing databases;
- creating new databases – including all required types of objects and connections;
- updating existing databases by adding new types of objects and connections as requirements arise;

- configuring databases by setting up code lists, labelling schemes and all the other things that affect how the database is used;
- administering databases by adding users, setting security, deleting old records and backing-up the data.

The roles of users include:

- adding, editing and deleting records;
- creating sets and queries;
- analysing the information by using a variety of analytical functions;
- creating reports and diagrams.

Link[29]

The Link environment is a comprehensive IT solution designed to support the work of criminal analysts. The basic version of the system offers a set of tools for integration, initial processing and visualisation of information from different sources, particularly phone call billings. Link is also a platform for integration of various methods of (semi-)automatic analysis of information which can be incorporated into the system as independent components.

Link provides for loading call billings and other graph data (tabulated) straight from original files. The ability or quickly import data with the use of defined templates allows analysts to load external data into the programme within seconds. The system comes with templates for importing phone call billings from all Polish mobile operators. Advances analysts can also create new templates and send them to other analysts, which allows for quickly adapting the application to changing data formats.

A set of analytical tools embedded in the Link environment allows analysts to conduct complicated operations by just a few mouse clicks. Such tools as intelligent linking of multiple billings to detect identical phone numbers and calls, unification of phone numbers1, call statistics or information filtering allow analysts to efficiently conduct analyses of mass data without the need to create large and unclear charts.

A key element of the Link environment is visualisation of billing and graph data on charts that show the structure of data interconnections. A set of various layouts of elements allows analysts to capture important data in various situations they meet in their everyday work. In addition, various views of the same data within a chart (e.g. structure of phone calls and relations between respective phone and IMEI numbers) allow the user to conduct various analyses without the need to re-import the same billing. Along with the editor functionality, Link offers a set of tools for creating final reports1 that become evidence in respective cases. The wide array of elements, advanced editing of visual properties and notes are examples of tools that allow analysts to easily create a chart so that it could present the analysis results in a clear manner. The Link environment is a comprehensive IT solution designed to support the work of criminal analysts. The basic version of the system offers a set of tools for integration, initial processing and visualisation of information from different sources, particularly phone

[29] A computer programme developed by the Intelligent Computer Systems Team of the Information Technology Department of AGH University of Science and Technology in Kraków, www: https://fslab.agh.edu.pl/ (10 May 2017).

call billings. Link is also a platform for integration of various methods of (semi-)automatic analysis of information which can be incorporated into the system as independent components.

Phases of analytical activities

Criminal analysis involves conducting activities in a structured order. In classical terms, the analytical cycle is a circle of activities which are repetitive and aimed at achieving final conclusions and a plan for further actions.

The course of an analysis has two phases: the first phase involves acquisition, selection and assessment of information, the second phase involves making investigation hypotheses regarding a specific case. An analyst can illustrate these hypotheses in many ways by presenting various scenarios (relating to past or future events) to support these hypotheses.

As an element of the information (intelligence) management process, criminal analysis consists of necessary phases of handling the information (case material) gathered. A fixed sequence of these phases can be distinguished although the fluently transition from to another and interpenetrate.

Review and selection of the material

The fact of reviewing the material gathered in a specific case may seem prosaic and appear to be merely the background for the analysis. However, one must notice the unique feature of such review that is rooted in the nature of the analysis itself – namely the careful reading and extremely detailed analysis of the facts. To embark on structuring and selecting the material, one must first review the material in its entirety. This applies to both to reading all case file sheets and recreating the data on other storage media (photographs, phone call billings, bank statements). An initial review of the entire material ensures proper planning of further analytical activities. It also allows the analyst to assess the material in terms of its completeness, trustworthiness (in relation to the sources and quality of information) and level of complication. In principle, an analysis should start with at least one review of the case without distracting one's attention to so-called „processing" of the material (like notes, selection etc.). Each subsequent reading provides for appropriate systematisation and proceeding to the next phase, namely selection. The material that is submitted for analysis is full of various types of unstructured factual data which require segregating. On reviewing the material, it must be „marked" i.e. data meant for further analysis must be extracted. The bulk of the material gathered is not too relevant to the case. This is due to the specific nature of specific documents/storage media (e.g. a memo, a witness interview report, CCTV footage), where only a small portion of the content has any information value. One may even venture to say that only a small portion of the material is valuable (in the context of utility in further analysis). The rest is just a text which a kind of a background. For instance, it is sufficient to note that often only a few paragraphs in a witness interview catch attention, while the rest does not contribute anything to the case whatsoever. Similarly, most of the documentation gathered in a specific case will not be taken into consideration, just like stenographic records of phone calls (if phone tapping was used) – which will offer little information useful for the analysis. Methods of selection can have different forms, depending

on the individual skills and qualifications of an analyst. It is practical to work on copies of the material, as it offers a greater freedom when working on paper documentation on which various notes can be made and fragments, even single sentences, highlighted. Using colours is a useful technique, as it facilitates reviewing the material when an analyst must get back to it. Finding persons, vehicles, addresses or company names in the text is easier when one decides to mark each of these with a separate colour. When working on the original, analysts can use sticky notes with relevant comments. However, electronic documentation is best for effective working on case materials (not only in terms of selection). Although digitalisation has become an inherent element of every criminal analysis, only selected material is digitised. At present, more and more data is stored electronically, which gives analysts this form of data at every phase of analysis, which is undoubtedly an advantage. Selected material is systematised further in a phase that can be called grouping.

Grouping and consolidation

Selecting data from the overall material accelerates its interpretation and reduces review time. However, the data is still unstructured and requires grouping. Segregating data or information (as a result of processing and interpretation of data) is natural in criminal analysis (or any other material analysis, for that matter). However, such segregation is not done

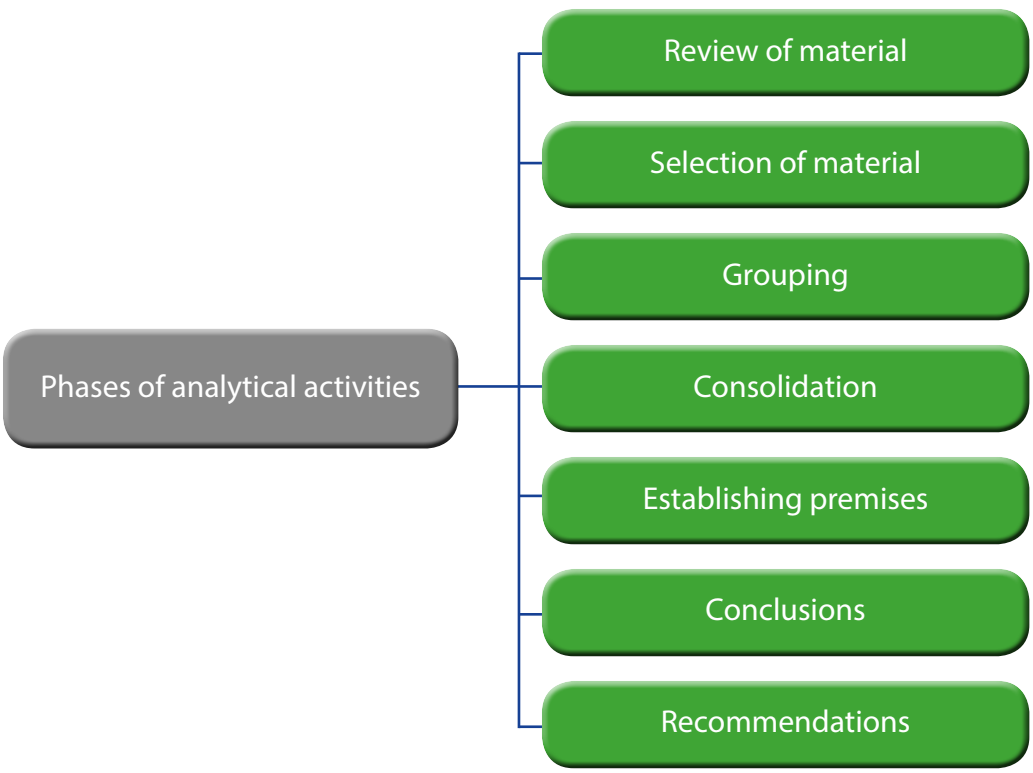


Figure 11. Phases of analytical activities (source: own research)

in a standard way, as it is determined by the nature of selected material and the independent decision of the criminal analyst. Data, information on a specific person or group of persons, information on a specific company in general or regarding circulation of documentation, transport, customer connections etc. all can be combined. Grouping of data and information in a database application, which is a tool in the analyst's arsenal, involves creating object and connection records. Objects will usually include e.g. a person, a bank account, a telephone number, an event, a document, an address, a company and many more as may be specific to the case. Connections have forms of specific relations e.g. an acquaintance, a capital relation, a phone call, a wire transfer, an owner, a user, a subscriber etc. At the same time, selected material is fed into a database where it will be segregated by object and connections types, and, thanks to analytical functions of the software used, will allow for quick formation of sets. And the sets are a result of a process of thought conducted by an analyst who „queries" the database for specific criteria. This activity is somehow a bridge between grouping and consolidation. Selection and grouping are the longest phases of analytical activities, and they may take the lion's share of the time planned for the analysis. However, they are the foundation for further analytical activities, which would be imperfect and unreliable if any mistakes were made at earlier phases. Analytical division of the material into elementary parts, selection of data important for the analysis and grouping the data open the way to its subsequent consolidation. Transition between grouping and consolidation is very fluid, so it is very difficult to delineate a strict border here. Consolidation takes place as a result of grouping data and information and compiling it according to specific criteria. It can take a graphic form in accordance with the analytical techniques mentioned above. An analyst can process data and information from various sources either in accordance with instructions (the objectives of the analysis provided in the request) or his or her own findings and ideas. Creativity of the analyst may become the key to success of the analysis, especially when working on a material where we are unable to capture all interdependencies using classical methods, even if we have the „reading-between-the-lines" skill. Tactically, it is best to consolidate the material and compile the data through the prism of connections and chronology of events observed in the case concerned. This offers the correct picture of the case and allows the analyst to proceed to further summaries (also analytical techniques, statistical tables) which will give grounds for the process of drawing conclusions. Consolidation of data takes place through a careful study of grouped information, diagrams and summaries, and it results in establishing relevant premises.

Establishing premises, drawing conclusions, giving recommendations

Premises are an important element of reasoning and affect the final shape of an analysis. Criminal analysis ends with conclusions and recommendations which must be supported by the case material. A set of grouped facts comprising the final conclusions are presented by the analyst in the form of a written or oral report in which the analytical process and logical reasoning must be reflected. Serving as a guide here can be premises that arise from the substance of the material and link facts in accordance with the grouping performed (data, information). In criminal analysis, a premise (expressed in one or a few sentences)

is a summary of a set of facts included in respective groups of data and information. Premises can by no means evolve into „small" conclusions. This would ruin the foundations of reasoning, for a conclusion (which in criminal analysis is treated as a version of events) cannot be based on other minor conclusions. Premises determine a subsequent structure of the final conclusions from the criminal analysis, which can take the form of e.g. an investigative version, a finding or a criminological forecast. A conclusion should be treated as a product of the analysis. Here, an association with marketing operations is well founded, for the process of obtaining an approval of an analyst's work by the recipient of the analysis can be brutally referred to as „selling the result of the analysis". If an analyst's work produces conclusions which give a specific case a new face, then the manner of formulating and explaining these conclusions (also by presenting scenarios), use of appropriate argumentation and, finally, convincing the recipient of the criminal analysis become extremely important. Even the best criminal analysis can be weakened if presentation of the conclusions (also thinking processes which led to those conclusions) is inappropriate, superficial or even distorted. Then the conclusions and recommendations may „end up in the background" of subsequent actions. Conclusions in a criminal analysis are based on, arise from and correspond to premises. They also cast new light on the case (a hypothesis, an investigative forecast). Premises support conclusions and represent the starting point for the process of reasoning. In criminal analysis, reasoning refers to the universal foundations of logic and is a manifestation of logical thinking. As every hypothesis, it must be verified to be proven. In criminal analysis, correlation between conclusions and premises consists in an appropriate selection of wording in the process of formulating both premises and conclusions.

If the material permits, conclusions should answer seven golden questions of forensics[30], otherwise they are not exhaustive. Their structure depends on the form in which they will be presented (oral, written). Criminal analysts are most often satisfied with a written report from the analysis in which conclusions normally have the form of sentences grouped in points. During an oral presentation of results, conclusions should be emphasised in a manner that will make the recipients remember the conclusions as the essence of the analysis. This effect cannot be achieved by using excessively complex sentences which are loaded with unnecessary content – one must always remember that a presentation of results of a criminal analysis is not an opportunity for speeches. Based on conclusions, an analyst prepares recommendations, which also are an important final product of each criminal analysis. One must remember that recommendations are not orders. Since an analyst suggests further actions and orients them, recommendations should be treated as proposals, indications regarding further actions. Although recommendations do not have a binding nature, one cannot say they are inapplicable. Each case is commissioned to an analyst for a reason, therefore recommendations are to pave the way to solving the problems underlying the request for analysis. In this light, rejecting or disregarding the analyst's suggestions would have to arise from an important reason (e.g. acquisition of new information changing the earlier findings).

[30] 1) What?; 2) Where?; 3) When?; 4) How?; 5) With what?; 6) Who?; 7) Why?, M. Kulicki, V Kwiatkowska-Darul, L. Stępka, *Kryminalistyka. Wybrane zagadnienia teorii i praktyki śledczo-sądowej*, Toruń 2005, p. 47.

Recommendations should contain non-categorical words like „would", „it is advisable", „it should be considered" etc. When formulating recommendations, one should avoid phrases associated with instructions or the imperative e.g. „execute", „interview", „complete", for they may arouse hostility to the analyst (who is to be considered a partner rather than a controller, and be associated with good cooperation rather than pointing out one's possible errors).

Although they close the phases of analytical activities, recommendations are created almost at every stage of the analytical process – some are formulated on an on-going basis as the analyst's ideas and defined (or recapitulated) at the end when all activities have been completed. The analytical process is concluded with presenting results of the analysis.

Use of criminal analysis by state security entities

Executing their statutory tasks, entities in charge of the State security use a number of instruments, including legal, organisational and technical ones. Among them is criminal analysis which, implemented in a number of entities, has evolved to cater for various directions of interest in some entities, while not finding any special recognition in others, which does not mean that the latter do not have analytical units which – when appropriately „motivated" – can in fact be useful in their operations.

Police as the pioneer of criminal analysis in Poland

The Police was the first service in Poland to systemically introduce criminal analysis to its structure and operations. Early models had been taken from police experiences in European countries long before Poland's accession to the European Union. Various activities related to combating organised and drug crime triggered development of EU standards for technical equipment and intelligence gathering, processing and exchanging procedures in EU Member States.

The British criminal intelligence and analysis system Alert was regarded a tool that met those requirements. In 2000, the Chief Commander of Police approved „The Programme for Implementation of Criminal Analysis" which included main assumptions regarding the future functioning of criminal analysis in Poland. The priority of that implementation strategy was development of appropriate personnel, investment and organisational base enabling the criminal intelligence and analysis system Alert. The system was envisaged to enable the Police to exchange, domestically and internationally, information according to uniform standards and establish cooperation with trained criminal analysts using the same analytical methods and techniques and IT tools when conducting operations in the country and abroad[31].

Actions listed in the aforementioned programme were aimed at three overlapping areas: training (educating the desired staff), investments (purchasing the equipment and software) and organisation (establishing structures and legal regulations enabling creation and effective

[31] Raport. nt. Analiza Kryminalna, Stan Aktualny i Plany Rozwoju, Biuro Służby Kryminalnej KGP, 2003.

functioning of analytical units within criminal intelligence)[32]. As can be seen, criminal analysis was implemented in The Police in three areas in parallel.

Training

The first group of 10 analysts were trained London in 1996, i.e. before the aforementioned criminal analysis implementation programme. Starting in 2000, the Police launched training in cooperation with the European Union. It was conducted at the Police Training Centre in Legionowo. During two training courses held as part of the Twinning'98, 24 operational analysts were trained, of whom European Union experts selected 6 candidates to become Polish trainers. Another training of 13 candidates for operational analysts was held in 2001. It was conducted by EU experts and the six Polish trainers selected earlier. As of the end of 2001, a total of 31 operational analysts had been trained (with the participation of EU experts). In the meantime, the management personnel in the field of criminal analysis were trained as part of various twinning programmes.

In line with „The Schedule of Implementation of Twinning'98 Recommendations", a criminal analyst training centre was launched at the Police Academy in Szczytno. In 2001, EU teaching materials were adapted to the needs of the Polish Police (based on trainings conducted by British trainers) and used for preparing the Polish operational analyst training programme. The first pilot training was launched in the same year, and regular training run only by Polish trainers started in 2002[33]. Apart from Police Academy lecturers, each four-week training course involved also criminal analysts from local units. Their participation in the training was meant to pass on the experience gathered in the area of operational analysis, which is practised to this day.

Several training cycles take place at the Police Academy every year, involving also services outside the Police – mainly the Border Guard and the Internal Security Agency, which started training their officers in 2003. The Police solutions and training facilities were also used by officers of, among others, the Military Counterintelligence Service, Central Anti-Corruption Bureau, Customs Service and prosecutor's offices.

Starting in 2001, the training involved not only criminal analysts alone, but also top and middle ranking staff and other police officers, mainly from crime and investigation teams. These training courses were initially aimed at promoting the concept of criminal analysis and, most importantly, making the community aware of the possibility to deploy criminal analysts in cases worked by the services. In October 2002, the National Symposium of Criminal Analysts was held with a view for improving the efficiency of external exchange of information and experience. Since then, the event has become cyclical and is held at the Police Academy in Szczytno every year.

Today, training courses for police analysts are held regularly at the Police Academy. In parallel, although this is a separate issue, selection of candidates for criminal analysts was put

[32] M. Hausman, *Implementation and development of criminal analysis in the polish Police*, [in:] Crime Intelligence RiskAssessment & Intelligence LedPolicing, CEPOL... op.cit., p. 30.

[33] J. Nęcki, *Analiza kryminalna. Stan aktualny i perspektywy*, [in:] *Policja Europy w XXI w. – w kierunku jakości. Materiały pokonferencyjne*, A. Letkiewicz i W. Pływaczewski (edit.), Szczytno 2003, p. 119 ff.

in place along with their referral to the aforementioned training courses. Selection of candidates was an important issue in the process of implementation of criminal analysis, and its details were incorporated in internal regulations within the Police force and subsequently implemented in other services.

Investments

In line with the adopted standard, two hardware and software solutions were purchased in 1997 with a view for testing their utility in the Police work. The purchase included five Autonomic Criminal Analysis Workstations (Polish: Samodzielne Stanowisko Analizy Kryminalnej, SSAK) with i2 Analyst's Notebook software which were deployed in four local Police units and the Police Academy in Szczytno.

In addition to that, and in line with the assumptions of „The Programme of Implementation of Criminal Analysis in Police Units", the system was adapted to the needs of Polish users in terms of:

– compliance with Polish law and the requirements established by the Polish Police,
– Polish language version of the software.

The hardware and software solutions then in place within the Alert system (with central installation at the former Organised Crime Bureau of the National Police Headquarters) were modified. Equipment for the nationwide criminal intelligence and analysis system was purchased in 2003 as part of the Phare 2000 pre-accession fund.

Investments made in following years focused on providing local Police units with access stations working with the system and ensuring sufficient working environment for the growing number of trained analysts (initially, they had to share their analytical workstations). In 2010, the Police had more than 200 Autonomic Criminal Analysis Workstations. Current investments are aimed at maintaining the equipment potential of the analytical workstations and ensuring updates of the analytical software. However, some local units still require more such workstations.

Organisation

The introduction of criminal analysis to Police operations and subsequent deployment of the broadly understood criminal intelligence system had to be preceded by appropriate organisational efforts. Done in many phases, the process required specific legislative and structural actions.

The priority was to ensure that all organisational units of the Police planned to conduct analytical tasks established their own criminal analysis components. After 2000, organisation of those components was uneven. Sometimes single criminal analysis positions were established, sometimes entire teams.

By 2003, criminal analysis components were prepared for the purpose of inclusion in the criminal intelligence process (in accordance European Union recommendations) in the following manner:

1) all units planned to conduct analytical tasks established their analytical components,
2) the components were given an interdisciplinary character,

3) the components received separate organisational status in the aspect of their future roles in criminal intelligence operations.

These organisational efforts provided for achieving specific advantages. The organisationally separate status allows the criminal analysis components to execute analytical tasks for the entire Police force, not only specific departments or services. Their interdisciplinary character favours execution of analytical tasks related to various types of crime, while the establishment of a central unit for coordination and supervision of criminal analysis activities has provided for maintaining the unity and cohesion of functioning and development of criminal analysis within the criminal intelligence process, and enabled its representation outside either directly or through other components.

Criminal analysis could not be a totally separate element of the Police work – its proper functioning has always been, and will always be, tied with the legal and organisational framework. Without appropriate implementation of system solutions, it would have been doomed to fail. It must be noted, however, that those system solutions have not been uniform as they evolved to create the contemporary picture of criminal analysis in the Police force.

Border guard and national revenue service

Boarder Guard

In accordance with legislation[34], the Border Guard (Polish: Straż Graniczna, SG) is a homogeneous, uniformed and armed formation established to protect the State borders, control border traffic and prevent and counter illegal migration.

Following Poland's accession to the Schengen Zone, the Border Guard was tasked with, mainly, protecting the border between the European Union and Russian Federation, Ukraine, Belarus and at international airports, as well as running operations related to combating illegal migration within the Republic of Poland[35].

The main tasks imposed on the Border Guard are therefore protection of the „green" border and control of traffic at border crossing points. But these are not the only areas of SG operations. The broad scope of the formation's responsibilities includes, among others, intelligence, preventions and detection of crimes and offences and prosecution of perpetrators (within the remit assigned to the SG) as well as gathering and processing information, especially regarding protection of the State borders, border traffic control, prevention and countering of illegal migration and providing such information to competent State authorities. As can be seen, some of the tasks imposed on the SG are characteristic of intelligence activities, and therefore tend towards analysis of information, also criminal analysis.

Analytical efforts taken within this service include strategic and criminal operational analyses. At the central level, the SG has two analytical departments which are situated in separate divisions i.e. the Criminal Operational Analysis Department in the Operations and

[34] The Act of 12 October 1990 on the Border Guard (Journal of Laws 1990, No. 78, Item 462).

[35] More information can be found on the Ministry of Interior website at https://www.msw.gov.pl/pl/aktualnosci/10301,Nowy-model- funkcjonowania-Strazy-Granicznej.html; content as of 18 March 2017.

Investigation Office and the Analysis Department in the Commander-in-Chief Headquarters; there are also risk analysis units in individual local branches[36].

In accordance with the SG internal regulations[37], criminal operational analysis (Polish: kryminalna analiza operacyjna, KAO) is divided into supporting, accompanying and initiating parts.

- supporting criminal operational analysis consists in conducting ad hoc and one-off analyses commissioned at various stages of operational cases or preparatory procedures and aimed at specifically defined objectives corresponding to those specific stages of operational cases or preparatory procedures,
- accompanying criminal operational analysis consists in continuously conducting (as far as possible) an analysis commissioned under a single request, which can be submitted at various stages of an operational case or a preparatory procedure, with having a due regard to the development of that specific operational case or preparatory procedure,
- initiating criminal Operational analysis consists in conducting the analysis on the basis of all available sources to initiate new areas of operational and exploratory or investigative interest.

Despite certain differences in terminology, criminal operational analysis serves similar purposes as in the Police force and is based on a similar system of specialist training[38]and unified analyst resources, as a result of which analytical products in both services do not differ from each other[39].

The Border Guard has mechanisms that regulate information management. These include specifically applicable regulations setting out guidelines for acquisition (covert and overt), gathering, processing and providing information. These actions are supported by dedicated computer database resources which facilitate appropriate gathering, accountability and protection of information. Every SG officer who receives service-related information must document it,

---

[36] In accordance with the SG Headquarters (KGSG) guidelines, risk analysis covers all activities aimed at identification of elements, characteristics and structure of specific phenomena and interconnections between them in order pinpoint the lacks and deficiencies in the border protection and management system (which includes, specifically, all activities related to the protection of the borders, control of border traffic and functioning of the formation) and identify ways to eliminate or limit the impact of these lacks and deficiencies on the achievement of the objectives; components of this analysis include threat assessment and risk assessment; Guidelines No. 189 of 29 September 2006 of the Chief Commander of the Border Guard on conducting risk analysis in border units of the Border Guard (Official Journal of KGSG, 2006, No. 8, Item 68).

[37] Regulation 26 of 15 April 2013 of the Chief Commander of the Border Guard on conducting of criminal operational analysis and electronic processing of criminal information by the Border Guard (Official Journal of KGSG, 2013, Item 33).

[38] Some SG criminal analysts have been trained at the Police Academy in Szczytno.

[39] According to § 12 of Regulation No. 26 of the KGSG, a criminal analyst should, as part of KAO activities: „1) comprehensively process information gathered in materials subject to KAO; 2) utilise information gathered in the Central Criminal Analysis Database „Analityk" and other available databases; 3) employ analytical methods and techniques and analytical software that are adequate to the KAO objective concerned; 4) cooperate, on an ongoing basis, with the office requesting KAO; 5) consult the officer requesting KAO on own initiatives regarding additional source materials in order to avoid duplication of such activities; 6) create analytical reports or other forms of presentation of the results in a manner that provides for identifying further actions in analysed operational cases or preparatory procedures"; Regulation No. 26 of 15 April 2013 of the Commander-in-Chief of the Border Guard...., op. cit.

and the nature of the information determines the specific computer resource in which it will be stored (e.g. information on border checks, operational information and other).

SG officers with access to the database resources use the information for service purposes; also analysts have a defined access to those resources as part of their analytical responsibilities. Processing of the information leads to creation of various documents, also analytical ones, which aggregate the knowledge used at the tactical (on-going cases) and decision-making (strategic) level.

Analytical products include reports from criminal operational analyses (conducted at the operations and investigation level), phenomenon analyses (e.g. crimes committed by foreigners), risk analyses (e.g. main trends in risks identified by the Border Guard in a given year, developed at the SG Commander-in-Chief Headquarters). Recipients of criminal analyses include officers who commission them, whereas phenomenon analyses and risk analyses are addressed to the SG management. In order to familiarise other SG officers in local units – in accordance with the superiors' instructions and depending on the needs and the content of the analyses – they are distributed further e.g. published on the SG website.

National revenue administration

The tasks of the National Revenue Administration, established in 2017[40] as a result of amalgamation of the Customs Service, tax administration and revenue control, are defined under the provisions of the Act of 16 November 2016 on the National Revenue Administration and executed through organisational units in the office of the Minister competent for public finance, revenue administration chambers, customs and revenue offices and revenue authorities. The National Revenue Administration executes its tasks by initiating audit activities and conducting preparatory procedures in accordance with the provisions of the Act of 6 June 1997 on the Code of Criminal Procedure[41], the Penal Fiscal Code and the Act of 24 August 2001 on the Code of Procedure for Violations[42] as part of customs, audit, tax or administrative procedures.

The process of implementing criminal analysis took place under the Customs Service and is described as such in this paper.

Analytical activities within the service have focused mainly on risk analyses in the Customs Service specific areas of interest. Similarly to the Police and other services, activities conducted by the Customs Service concentrated on gathering and processing information where analysis (also risk analysis) played an important role. The Customs Service have not used criminal analysis in its operations, which significantly reduced its ability to combat crime – especially fuel, drug, alcohol, tobacco and gambling crimes – and conduct e-control through the Internet. This is why the service has become more interested in implementing criminal analysis.

[40] The Act of 16 November 2016 on the National Revenue Administration (Journal of Laws 2016, Item 1947).

[41] Code of Criminal Procedure (Journal of Laws 1997, No. 89, Item 555, as amended).

[42] The Act of 24 August 2001 – the Code of Procedure for Violations (Journal of Laws 2001, No 106, Item 1148).

Under a decision of the Head of the Customs Service, the service established the Task Team for Implementing and Functioning of Criminal analysis in the Customs Service[43]. A concept was developed for implementing criminal analysis in the Customs Service, which included proposals of solutions regarding a new analytical mechanism to support operations of this service. The mechanism will ensure increasing, and subsequently maintaining the high level of statutory performance of the Customs Service in the areas of identifying, detecting, preventing and combating of crime within the remit of the Customs Service. Application of criminal analysis as a tool supporting Customs Service operations is in line with the process of changes that are aimed at adapting the Customs Service to effectively combat the threats. Also, there are plans to restructure respective crime units and change their operating rules, which is expected to ensure further improvement of the service's performance[44].

Activities conducted with the use of criminal analysis have been identified in the Concept for Implementation and Functioning of Criminal Analysis in the Customs Service (Polish: *Koncepcja wdrożenia i funkcjonowania analizy kryminalnej w Służbie Celnej*), in accordance with they shall ensure:

- precise focusing of control activities conducted by crime combat units with respect to entities and individuals that may be connected with criminal activity,
- supply of information that requires further refinement and confirmation by e.g. surveillance under Article 75b of the Act on the Customs Service and exploratory and operational activities under Article 75c of the said Act,
- ability to create and verify investigative hypotheses in preparatory procedures conducted by officers of investigation teams,
- guidance regarding specific criminal events and ability to identify individuals and crime groups behind those events, mechanisms of their operations and structures in which they operate,
- cooperation with other services involved in combating organised crime. It should be noted that the process of implementation of criminal analysis in the Customs Service was based mainly on Police experiences and knowledge, which permitted a professional and appropriate approach to the subject in all areas. This applied to organisation (particularly the roles and situation of criminal analysts within the Customs Service), training (appropriate definition of the training needs and methods) and investments (selecting adequate hardware and software). The cooperation established at implementing criminal analysis in the Customs Service is now continued by holding joint professional training courses, seminars, conferences and exchange of experiences, which has a positive effect on the high level of skills of criminal analysts. The cooperation brings many advantages, starting from improving analysts' qualifications through to unification of their „arsenal", which translates to the ease of exchange and flow of information.

[43] Decision No. 18/SC of 6 November 2012 of the Head of the Customs Service regarding the establishment of the Task Team for implementation of criminal analysis in the Customs Service.

[44] *Koncepcja wdrożenia i funkcjonowania analizy kryminalnej w Służbie Celnej*, unpublished document, 2013.

Role of criminal analysis in special services

Effective special services are in many ways extremely important to the State security. Their operations are related to combating international terrorism, organised crime, proliferation of weapons of mass destruction and means of their delivery as well as counterintelligence protection, economic security of the State and protection of classified information. Such wide spectrum of special services' responsibilities is a result of modern day threats to the State security which require both proactive and reactive approach. The bond that links activities of special services is the need to ensure continuous intelligence support to the State depending on individual tasks imposed on them.

These services acquire, gather and process information related to the internal and external security of the Polish State (in the immediate neighbourhood, within Europe, the Euro-Atlantic zone and globally). The play a role in protection of Polish civil and military contingents on foreign deployments. They must identify (analyse) the situation, as it develops, in various parts of the world where there are terrorist attacks, conflicts, tensions or crisis situations (internal or international).

In order to control activities of Polish special services, the Special Forces Committee was established at the Council of Ministers which provides opinion and advice on matters of programming, supervision and coordination of the operations of the ABW, AW, Military Counterintelligence Service, Military Intelligence Service and Central Anti-Corruption Bureau as well as actions taken to protect the State security by the Police, Border Guard, Military Police, Prison Service, Government Protection Bureau, Customs Service, revenue authorities, revenue chambers, tax control authorities, financial information authorities and intelligence services of the Polish Armed Forces.

Some special service operations include certain analytical activities which, despite their unique nature, permit application of criminal analysis in its original form. It is therefore appropriate to review the nature of special service operations, having regard to the analytical activities they perform in the context of application (or possible application) of criminal analysis. It is also important to emphasise the solutions which have evolved throughout the period of use of criminal analysis or solutions that can be used as their replacement in Poland's special services. Poland's special services include the Internal Security Agency, the Intelligence Agency, the Military Counterintelligence Agency, the Military Intelligence Agency and the Central Anti-Corruption Bureau.

Internal Security Agency (ABW)

The Internal Security Agency (Polish: Agencja Bezpieczeństwa Wewnętrznego, ABW) was established under the Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency (both services replaced the Office for State Protection, established in 1990).

As the service competent for the protection of the State internal security and the constitutional order of the State, the ABW has the widest scope of actions and responsibilities of the five Polish special services. Some of them – like civilian counterintelligence, combating terrorism within the Republic of Poland, preventing proliferation of weapons of mass destruction

and means of their delivery as well as protection of classified information in international relations – are assigned solely to this Agency.

As part of its operations, the Internal Security Agency conducts analytical and intelligence activities, exploratory and operational activities, procedural activities, activities related to the process of protection of classified information, and it gives its opinions on relevant matters. It operates through departments, offices, 16 delegations and other organisational units.

Analytical and intelligence activities conducted by the ABW consist in acquisition and processing of information important to the protection of the State's internal security and the constitutional order of the State, and important for the position of our country on the international scene. The activities are reported to the President of the Republic of Poland, the Prime Minister and member of the Council of Ministers. Reports filed in 2012 regarded, among others, threats to economic foundations of the country; threats from foreign special services and counterintelligence protection of vital sectors of the national economy; terrorist threats, including new trends in Islamic terrorism and extremist groups; existing of forecast threats to the State's internal security and the constitutional order of the State, including threats arising from foreign and internal policies of states whose strategic interests might be in conflict with Polish interests[45].

Operational and exploratory activities conducted by the ABW are closely related to executions of the Agency's statutory tasks. They include legally permitted covert acquisition of information on individuals, locations or events that are important to the internal security of the Republic of Poland.

Procedural activities conducted by the ABW include detection of espionage, terrorism, breaches of the state secrets and other crimes against the State security and economic foundations of the State, as well as corruption among public officers308, crimes regarding production and trade of goods, technologies and services of strategic importance to the State security, illegal production, possession and trade of weapons, ammunition and explosives, weapons of mass destruction, drugs and psychotropic substances in international trade, and prosecuting perpetrators of those crimes. ABW officers conduct also other activities aimed at identifying locations of perpetrators who are evading law enforcement services.

The scope of the Agency's activities is closely related to acquisition, gathering and processing of information. One can notice the role of information analysis, specific to services of this type, which allows it to quickly provide processed information to State decision-makers. It is also important to note that the ABW employs criminal analysis (within the scope described in this paper), which in the case of the Agency's exploratory and operational activities and procedural activities should, in most cases, be similar to that employed by the Police (e.g. „fuel" cases).

Central Anti-Corruption Bureau (CBA)

Corruption is a threat to every state's law order, economy and the entire democratic system. It also very complex and has many forms. Corruption and other real risks to the democratic being of the Republic of Poland were at the foundations of the decision to establish a separate

[45] https://www.abw.gov.pl/pl/zadania/analizy-i-informacje/51,Analizy-i-informacje.html

special service to deal with those phenomena. The Central Anti-Corruption Bureau (Polish: Centralne Biuro Antykorupcyjne, CBA) was established under the Act of 9 June 2006 which entered into force on 24 July 2006.

The CBA is therefore the special service (and at the same time a central office of the government administration) established specifically to combat corruption in public and economic life, in particular in the State and local authorities, and to combat economic activities that are against the State's economic interests.

The primary objective of the CBA is to combat corruption that appears at the contact point between the public and private sector. CBA operations include the following areas:

- exploratory and operational activities and investigation activities,
- control activities,
- analytical activities,
- corruption prevention (also anti-corruption education)[46].

Analytical and intelligence activities conducted by the Central Anti-Corruption Bureau are focused on identification of irregularities in and threats to the State's economic interest which, when detected, must be reported to the Prime Minister and other key State officials. Normally, these activities consist in systematic monitoring of public procurement, privatisation processes and selected government programmes. The analysis is aimed at initial identification of potential threats and preparation of a comprehensive assessment of the situation330.

Furthermore, the CBA may acquire and process data from resources – also personal data resources – kept by public authorities and as well as State and local organisational units[47]. Exploratory and operational activities and investigation activities conducted by the CBA involve criminal analyses whose character is not much different from tasks assigned to analysts in the Police and some other services.

CBA information analysts are situated in the Analyses Department and deal mainly with strategic/systemic and intelligence analysis. Their primary task is to identify serious corruption threats to the State's economic interest. Findings are reported to the key State officials listed in Article 2 Paragraph 1 Point 6 of the CBA Act. In their work, they use, among others, white intelligence (OSINT), internal and internal databases, classified information and criminal analyst tools. On the other hand, criminal analysts situated in CBA Delegation Offices deal primarily with analysing materials supplied by their superiors from operations and investigations departments (the so-called operational and procedural criminal analysis). Their role is primarily to support decision-making processes which determine CBA activities.

Criminal analysis is employed mass data is processed, particularly where it serves ensuring the State security. This applies to matters both in micro (event/case analysis) and macro scale (strategic/systemic analysis). As already mentioned, CBA information analysts often use criminal analyst tools in their strategic and intelligence analyses. Such compilation of various proven methodologies significantly improves their performance.

[46] https://cba.gov.pl/pl/o-cba/zadania/350,zadania.html

[47] Article 22 of the Act of 9 June 2006 on the Central Anti-Corruption Bureau (Journal of Laws 2012, Item 621).

Conclusion

State and administration authority in charge of internal security are faced with the dilemma related to making decisions regarding to both strategic and on-going matters. These decisions are made on the basis of information analysis. Each authority – with its own system of gathering, storing and processing of information – relies on relevant practices it developed within its structures.

Pioneered in Poland by the Police, criminal analysis is not only employed by majority of entities in charge of the State security, but it is also modified and adapted by them to fit their own needs. Those changes demonstrate that the solutions in service to date are being developed. Apart from the Police, which is the chief user, entities that use criminal analysis include special services of the Republic of Poland, which employ criminal analysis in certain areas and use criminal analysis tools in others. Furthermore, other entities like the Customs Service and its successor, the National Revenue Administration, are launching comprehensive implementation of criminal analysis in their operations. Also, various criminal analysis solutions can evolve and be combined, as can their adaptation in other areas where it has not been employed to date e.g. like with special services and their analytical and intelligence activities and strategic reports. Criminal analysis mechanisms can also be used outside State structures in the private sector, mainly by banks and insurers, which are exposed to risks related to the functioning of the financial and insurance markets.

An important direction of a broader utilisation of criminal analysis in the future will include actions related to gathering and processing of large volumes of information regardless of their nature, also by entities which have not employed criminal analysis before.

Criminal analysis will, naturally, have more space in which to evolve in all directions – from a broader use within the aforementioned security-related entities to an ever increasing number of those entities. Criminal analysis is an instrument which can be used almost universally, but it also can be easily modified and adapted to specific needs without losing its unique advantages.

References

Analiza kryminalna (uaktualniona wersja 2.0.), przekład G. Butrym, Legionowo 1999.
Analiza kryminalna, internal study (not published) KGP, 2004 r.
Chlebowicz P. i Filipkowski W., *Analiza kryminalna aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2011.
Gołębiowski J., *Profilowanie kryminalne*, Warszawa 2008
Hanausek T., *Kryminalistyka. Zarys wykładu*, Kraków 2000
Hausman M., *Implementation and development of criminal analysis in the Polish Police, [in] Crime Intelligence Risk Assessment & Intelligence Led Policing*, CEPOL, Warszawa 2010.
Hołyst B., Kube E., Schulte R., *Przestępczość zorganizowana w Niemczech i w Polsce. Zwalczanie i zapobieganie*, Warszawa 1998
Huzior-Kamińska A., *Medycyna sądowa w służbie profilowania kryminalnego sprawców zabójstw*, [in:] J. Ignaczak W., Michna P., *Analiza kryminalna*. *Zarys wykładu*, Szczytno 2002.
Ignaczak W., *Wybrane zagadnienia analizy kryminalnej*, Szczytno 2005.
Informator o Centralnym Biurze Antykorupcyjnym, Warszawa 2012
Instrukcja Stosowania Analizy Kryminalnej w Służbie Celnej
Kobylas M. *Zastosowanie analizy kryminalnej w zwalczaniu cyberterroryzmu*-a research paper
Kobylas M., Hausman M., *Problemy funkcjonowania analizy kryminalnej w Polsce w kontekście aktualnych rozwiązań i doświadczeń*. Report from the III Criminal Analysts Symposium (Szczytno, 8-10 November 2004). „Police", nr 4 z 2004
Kulicki M., Kwiatkowska-Darul V, Stępka L., *Kryminalistyka. Wybrane zagadnienia teorii i praktyki śledczo-sądowej*, Toruń 2005
Korzeniowski L. F., *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, Kraków 2008
Olender-Skorek M., Wydro K. B., *Wartość Informacji, Telekomunikacja i Techniki Informacyjne*, tom nr 1-2/2007, Warszawa 2007
Liedel K., *Profilowanie sprawców przestępstw terrorystycznych, [in:]* J. Konieczny, M. Szostak (edit.), *Profilowanie kryminalne*, Warszawa 2011.
Nęcki J., *Analiza kryminalna. Stan aktualny i perspektywy*, [in:] *Policja Europy w XXI* w. – *w kierunku jakości. Materiały pokonferencyjne*, red. A. Letkiewicz i W. Pływaczewski, Szczytno 2003
Report on operations of the Internal Security Agency in 2012, Warszawa 2013.
Raport. nt. Analiza Kryminalna, Stan Aktualny i Plany Rozwoju, Biuro Służby Kryminalnej KGP, 2003

Legal sources

The Act of 16 November 2016 on the National Revenue Administration (Journal of Laws 2016, Item 1947).
The Act of 24 July 1999 on the Customs Service (Journal of Laws 1999, No. 72, Item 802).
The Act of 24 August 2001 – the Code of Procedure for Violations (Journal of Laws 2001, No 106, Item 1148).
The Act of 27 August 2009 on the Customs Service (Journal of Laws 2009, No. 168, Item 1323).

The Act of 6 June 1997 – the Penal Code (Journal of Laws 1997, No. 88, Item 553).
The Act of 9 June 2006 on the Central Anti-Corruption Bureau (Journal of Laws 2012, Item 621).
Regulation 1012 KGP of 23 September 2004 on the use of criminal analysis by the Police (Official Journal of KGP, 2004, No. 20, Item 124).
Guidelines No. 189 of 29 September 2006 of the Chief Commander of the Border Guard on conducting risk analysis in border units of the Border Guard (Official Journal of KGSG, 2006, No. 8, Item 68).
Regulation 26 of 15 April 2013 of the Chief Commander of the Border Guard on conducting of criminal operational analysis and electronic processing of criminal information by the Border Guard (Official Journal of KGSG, 2013, Item 33).

Electronic sources

http://www.antykorupcja.gov.pl/ak/instytucje-antykorupcy/wyspecjalizowane/w-Polsce/
https://www.abw.gov.pl/pl/zadania/analizy-i-informacje/
http://analitycy.org/
https://cba.gov.pl/
http://www.wspol.edu.pl/d/archiwum/389-22-24-wrzepnia-miynarodowe-seminarium-analitykkryminalnych

Andrew Tennant

Money Laundering Investigation Team, North East Regional Asset Recovery Team, UK

Crypto Currency (Bitcoin) – guide for search officers

Abstract

Is Bitcoin the new currency for crime?

Across the globe there has been an increased number of ransomware attacks with an outlaying demand for payment in Bitcoin. The use of crypto currency in making cross boarder and international payments within the world of crime is on the increase. Is Bitcoin the emerging threat that we are now seeing organised crime utilising? This presentation is intended to explain some aspects of cryptocurrency, its features, how it is exploited by organise crime and how law enforcement organisations and institutions can look to intercept and recover.

What is bitcoin?

Bitcoin is a digital currency. It is essentially a piece of code that can be used to store and transfer value. Bitcoin is not illegal; it can be used legitimately and is done so by millions of people across the world. The Bitcoin network and its popularity continue to rise. It is here to stay and due to its decentralized nature and the fact it is unregulated, it's impossible to ever "shut down".

Why do i need to know about bitcoin?

All search officers know what a pile of cash looks like; police regularly seize cash under POCA and PACE legislation. However the criminal use of Bitcoin presents new challenges to law enforcement: a piece of code can be used to store and transfer an infinite amount of money, and in the digital age, officers need to know what to look for.

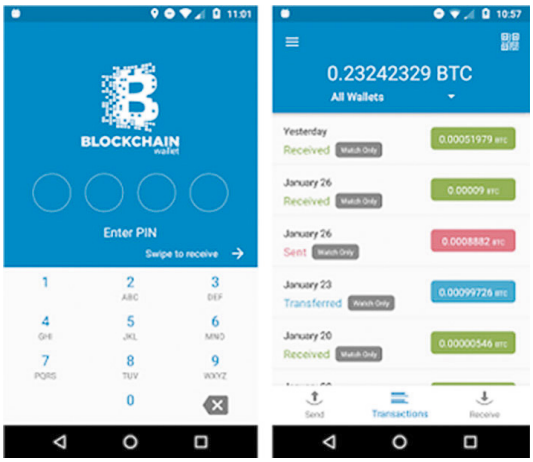
How does it work?

A process called public key cryptography. This is too complicated to explain here; all you need to know is that if you own bitcoin, then people are willing to pay you money for it. For more information there are various websites available explaining the technology in detail – see **bitcoin.org** and **coindesk.com** for more info.

Importantly, every transaction that has ever taken place using Bitcoin is available on a public ledger known as the blockchain. Therefore, if you have a bitcoin address you can check how many bitcoins are stored there. See **www.blockchain.info** for more detail.

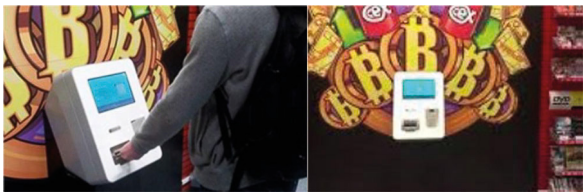
How do people buy bitcoin?

The easiest way is to download a bitcoin wallet app on your phone, two of the most popular are blockchain.info and Coinbase. Once downloaded, the app can then generate a bitcoin address.



A mobile wallet can effectively be used as a bank account. Once you have a bitcoin wallet you can buy bitcoin in one of three ways:

1. **Bitcoin ATMs** - You put cash in a machine, scan your phone and store the value in your bitcoin wallet.



2. **In person** – various websites are available whereby you can purchase bitcoin through a face to face transaction.
3. **Exchanges** – these are legitimate websites, you sign up and pay for bitcoin via either a bank transfer or with your credit / debit card - just as you would pay for your groceries. Many of these exchanges require you to provide copies of your identification.

How and why do criminals use bitcoin?

1. **To buy illegal goods on the dark web -** Bitcoin is the currency of choice on the dark web. You can sign up to websites and pay for drugs, firearms and other illegal goods using bitcoin.

2. **To store value (i.e. like a bank account)** – criminals find it difficult to store the proceeds of crime in their bank accounts. Bitcoin wallet apps can effectively be used as a bank account to store the proceeds of crime.

3. **To transfer money** – criminals can send substantial amounts of money across the world at the press of a button. Unlike traditional money transfer methods this is impossible to control and regulate and costs just a few pence. Bitcoin is often a requested payment method for online crimes such as Sextortion and Ransomware.

How and where are bitcoin stored?

1. Electronic device (phone, laptop etc.)
2. Paper wallet
3. **Hardware wallets**

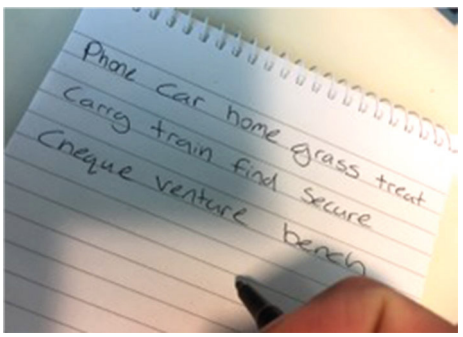
The majority of bitcoin related activity will be conducted on devices such as smart phones and computers and will therefore require a digital forensic examination however bitcoins can also be stored in a paper and hardware wallets.

What do paper wallets look like?

What do hardware wallets look like?

Popular Hardware Wallets include Trezor, Ledger and Keepkey. These devices can be used to store bitcoins. They have an extra level of security so keep a look out for passwords, notebooks or "seeds".

What is a seed? This is what appears to be a random set of words either 12, 18 or 24 in length. In basic terms the seed can be used to back-up a suspect's bitcoin (it is a human readable interpretation of your private key).



What else do i need to look for?

Bitcoin addresses - A bitcoin address is an alpha-numeric code of between 26-35 characters (most are 33) that begins with either a 1 or 3. Bitcoin addresses can also be visualised as QR codes (see the black and white squares)

Private keys - In order to control the bitcoin (i.e. have the ability to sell it or transfer it) you need to know the private key (this is generated when the bitcoin address / public key is generated. The private keys are either 51 or 52 alpha-numeric characters that usually begin with 5, L or K (see examples below).

5Kb8kLf9zgWQncgidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF

Can you seize bitcoin?

If you control the private key then you control the bitcoin in the public address. All paper wallets, electronic devices and notepads should be seized as evidence under section 19 of PACE. POCA legislation can also be used

If a suspect is arrested and then bailed, it is likely that they or their associates, have online back-ups of their private keys, and could transfer the bitcoin to a new address. It is imperative that you speak to a Bitcoin SPOC ASAP to seek advice regarding seizure. It may be possible to transfer the bitcoin to a police controlled wallet to prevent the dissipation of funds.

Andrew Tennant
Money Laundering Investigation Team, North East Regional Asset Recovery Team, UK

Kryptowaluta (bitcoin) – informacje dla funkcjonariuszy prowadzących przeszukania

Abstract
Czy bitcoin jest nową walutą przestępców?
Na całym świecie wzrosła liczba ataków dokonywanych przy pomocy oprogramowania ransomware, w których przestępcy żądają zapłaty w zamian za odszyfrowanie dysku w bitcoinach. Coraz powszechniejsze staje się stosowanie tak zwanych kryptowalut w celu dokonywania płatności transgranicznych i międzynarodowych w przestępczym półświatku. Czy bitcoin jest nowym zagrożeniem, z którego obecnie korzysta przestępczość zorganizowana? Prezentacja ta ma na celu wyjaśnienie niektórych aspektów kryptowalut, ich cech, sposobu, w jaki są one wykorzystywane przez organizacje przestępcze oraz sposobu, w jaki organy i instytucje odpowiedzialne za egzekwowanie prawa mogą próbować przechwycić i odzyskać majątek przenoszony przy pomocy kryptowalut.

Czym jest bitcoin?

Bitcoin (BTC) jest walutą cyfrową, nazywaną także czasem kryptowalutą. W praktyce jest to kod, który może być wykorzystywany do przechowywania i przenoszenia wartości. Bitcoin **nie jest** nielegalny; jak każda waluta może być wykorzystywany do legalnych celów i robią to codziennie miliony ludzi na całym świecie. Sieć bitcoin stale się rozwija, a popularność waluty rośnie na całym świecie. Bitcoin stał się jedną z używanych walut, a z racji jego zdecentralizowanego charakteru i braku jakichkolwiek regulacji niemożliwe jest wyłączenie sieci i likwidacja waluty.

Do czego potrzebna mi jest wiedza na temat tej waluty?

Wszyscy funkcjonariusze wiedzą doskonale jak wygląda duża ilość gotówki; Policja bardzo często konfiskuje gotówkę na mocy ustaw POCA oraz PACE. Fakt, że przestępcy zaczęli używać kryptowalut takich jak bitcoin stanowi nowe wyzwanie dla organów ścigania, ponieważ obecnie niewielki kod może zostać wykorzystany do przechowywania i przenoszenia dowolnej kwoty. Z tego powodu funkcjonariusze muszą wiedzieć, czego szukają i z czym mają do czynienia.

Jak działa bitcoin?

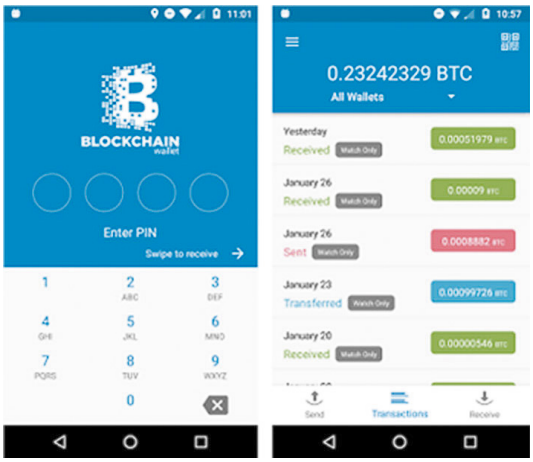
Bitcoin opiera się na procesie zwanym kryptografią klucza publicznego. Proces ten jest zbyt złożony by wyjaśnić go w tej broszurce. Najważniejszy jest fakt, że bitcoin posiada dużą wartość i są osoby skłonne zapłacić za tę walutę realną gotówką. Więcej informacji na temat

samej waluty, a także związanej z nią terminologii można znaleźć na witrynach internetowych takich jak np. **bitcoin.org** oraz **coindesk.com**.

Przede wszystkim jednak każda transakcja, która kiedykolwiek miała miejsce jest zapisana w publicznym rejestrze znanym pod pojęciem „blockchain". Tym sposobem po uzyskaniu adresu portfela bitcoin możliwe jest sprawdzenie jak wiele BTC jest przechowywane w danym portfelu. Więcej informacji można znaleźć na stronie **www.blockchain.info**.

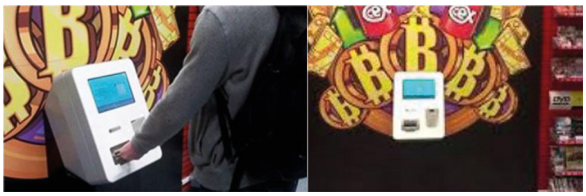
W jaki sposób ludzie kupują BTC?

Najprostszym sposobem jest pobranie aplikacji, tzw. portfela bitcoin na telefon – dwie najpopularniejsze aplikacje to blockchain.info oraz Coinbase. Po pobraniu aplikacja może wygenerować adres portfela bitcoin.



W praktyce mobilny portfel może być wykorzystywany jako konto bankowe. Po stworzeniu portfela możliwy jest zakup BTC na jeden z trzech sposobów:

1. **Bankomaty BTC** – po umieszczeniu gotówki, maszyna skanuje kod na ekranie telefonu, a następnie przekazuje zdeponowaną wartość do portfela.



2. **Osobiście** – w Internecie dostępne są witryny umożliwiające zakup BTC bezpośrednio od innej osoby.

3. **Kantory BTC** – legalnie działające witryny internetowe, z których po rejestracji można skorzystać w celu zakupu BTC przy pomocy przelewu bankowego lub płatności kartą kredytową / debetową, podobnie jak na przykład za zakupy internetowe. Wiele spośród działających kantorów wymaga okazania kopii dowodu tożsamości.

W jaki sposób i dlaczego przestępcy używają BTC?

1. **W celu zakupu nielegalnych towarów na internetowym czarnym rynku** – bitcoin jest ulubioną walutą przestępców operujących na internetowym czarnym rynku. Istnieją witryny internetowe, które po rejestracji umożliwiają zakup narkotyków, broni oraz innych nielegalnych towarów i zapłatę przy pomocy BTC.

2. **W celu przechowywania wartości (zamiast konta bankowego)** – wielu przestępców styka się z trudnościami z przechowywaniem środków finansowych pochodzących z przestępstw na kontach bankowych. Portfele bitcoin mogą być skutecznie używane jako konta bankowe służące do przechowywania pieniędzy uzyskanych w wyniku popełnionych przestępstw.

3. **W celu przekazywania pieniędzy** – korzystając z kryptowalut takich jak BTC przestępcy mogą z łatwością przesyłać duże ilości pieniędzy do dowolnego miejsca na świecie. W przeciwieństwie do tradycyjnej gotówki przelewy przy pomocy BTC są niemożliwe do kontrolowania i regulacji przy pomocy przepisów, a dodatkowo są także niezwykle tanie. Bitcoin jest bardzo często wymaganą metodą płatności w przypadku przestępstw internetowych, takich jak szantaże oraz ataki przy pomocy oprogramowania typu ransomware.

W jaki sposób i gdzie przechowuje się BTC?

1. Na urządzeniach elektronicznych (telefonie, laptopie itd.).
2. W portfelu papierowym.
3. **W portfelu sprzętowym.**

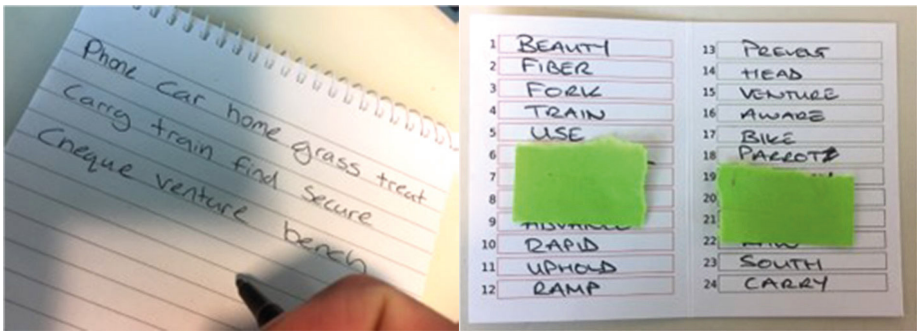
Większość działań związanych z BTC jest prowadzona przy pomocy urządzeń takich jak smartfony i komputery, z tego powodu konieczne będzie ich sprawdzenie przez biegłego ds. informatyki śledczej. Dodatkowo jednak BTC mogą być przechowywane w portfelach papierowych i sprzętowych.

Jak wyglądają portfele papierowe?

Jak wyglądają portfele sprzętowe?

Wśród popularnych portfeli sprzętowych można wymienić między innymi urządzenia Trezor, Ledger oraz Keepkey. Wszystkie spośród tych urządzeń mogą posłużyć do przechowywania BTC. Urządzenia te charakteryzują się dodatkowymi zabezpieczeniami, dlatego warto o tym pamiętać w czasie przeszukania i zwrócić uwagę na wszelkie hasła, notatki lub wartości bazowe (tzw. seed).

Czym jest wartość bazowa? Wartość bazowa wygląda na pierwszy rzut oka jak losowy ciąg słów zawierający 12, 18 lub 24 słowa. Ogólnie rzecz ujmując wartość bazowa może zostać wykorzystana do wykonania kopii zapasowej portfela podejrzanego – w praktyce jest to wersja klucza prywatnego możliwa do odczytania przez człowieka.



Na co jeszcze należy zwrócić uwagę?

Adresy bitcoin – to kod alfanumeryczny składający się z 26-35 znaków (większość zawiera 33 znaki), zaczynający się liczbą 1 lub 3. Adresy bitcoin mogą być także przedstawiane w formie kodu QR (biało-czarne kwadraty).

Klucze prywatne – aby mieć pełną kontrolę nad walutą (tj. mieć możliwość jej sprzedaży lub przekazywania innym osobom), wymagana jest znajomość klucza prywatnego (generowanego w tym samym czasie, w którym generowany jest klucz publiczny – adres bitcoin). Prywatne klucze zawierają zazwyczaj 51 lub 52 znaki alfanumeryczne, rozpoczynające się cyfrą 5, bądź literami L lub K (zobacz przykłady poniżej).


```
5Kb8kLf9zgWQncgidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF
```

Czy możliwe jest skonfiskowanie BTC?

Kontrolując klucz prywatny jesteś posiadaczem wszystkich BTC przypisanych do danego klucza publicznego. Wszystkie portfele papierowe, urządzenia elektroniczne oraz notatniki powinny zostać zatrzymane jako dowody w sprawie zgodnie z art. 19 PACE. Można w tej sytuacji wykorzystać także przepisy POCA.

Jeśli podejrzany zostanie aresztowany, a następnie zostanie wpłacona kaucja, istnieje duże prawdopodobieństwo, że inne osoby miały kopie klucza prywatnego i były w stanie przesłać BTC na inny adres. Z tego powodu należy skontaktować się z osobą zajmującą się BTC tak szybko jak to możliwe, aby uzyskać informacje i porady na temat konfiskaty. W niektórych przypadkach może istnieć możliwość przesłania BTC do portfela kontrolowanego przez organy ścigania, aby zapobiec możliwości przekazania lub wypłacenia środków.

Brian Ludlow

Economic Crime Command, National Crime Agency, UK

Trade Based Money Laundering (TMBL)

Abstract

TBML is probably the most wide spread form of money laundering today, moving potentially the largest volume of criminal proceeds throughout the world. Worryingly, it is also probably the form of money laundering which is least investigated or avoided by Law Enforcement. The reason? It can be difficult and can take time. Accordingly, billions are laundered through TBML. TBML is the exploitation of trade to disguise the movement of criminal proceeds. The criminal monies are lost in the 'white noise' of the millions of trade deals which are conducted globally. TBML can: move value without physically transferring money; breaks audit trails; disguises Beneficial Ownership; can facilitate other crime such as tax and currency controls. TBML can come in many forms. This presentation is intended to explain some aspects of TBML, its features and how to recognise it. Importantly it seeks to develop methods to combat this problem.

"Money laundering" is often understood to mean those actions taken by a criminal (or a group of criminals) to "clean" money which has been obtained through criminality, in order that it can be freely used without detection or apprehension. The term itself actually has a much wider meaning.

It is frequently asserted that most crime is motivated by financial gain. Accordingly, financially motivated crime will (if successful) generate the proceeds of that crime (hence the technical term 'proceeds of crime'). The proceeds of a crime may not necessarily be merely a cash concept, but would also include the assets generated by a criminal act. The processes of acquiring, possessing, concealing, using, or otherwise controlling the proceeds of crime are all known as money laundering. This popular definition is repeatedly referred to in government legislation across the globe, amongst fiscal regulatory regimes, and also amongst academics.

Generally one of the first tasks of a criminal when he obtains the proceeds of crime is to ensure that it is safe. The criminal will want to be able to enjoy these proceeds without arousing the suspicion of the Authorities, or others who may notify the Authorities, and therefore run the risk of arrest and/ or having these proceeds of crime taken away by the Authorities. Accordingly, the criminal will launder the proceeds to enjoy the benefits of the criminal activity.

In the UK, money laundering has been criminalised through a number of progressive acts of parliament. Technical money laundering activities include:

- Concealing, disguising, converting and transferring criminal property
- Removing criminal property from the jurisdiction
- Entering into arrangements to facilitate the acquisition, retention, use or control of criminal property
- Acquisition, use or possession of criminal property careful here as we wouldn't want to usurp the Judge's role, or be questioned too much in relation to the legislation itself in isolation…

Mounting Regulation and the registration of certain trade sectors vulnerable to exploitation by money launderers has also taken place. The 'Regulated Sector' (needs some further explanation for the man in the street) is required to seek information from their customers to explain transactions, to critically examine those transactions to ensure there are not any suspicions of money laundering, and to disclose on suspicious transactions – such suspicions are reported to NCA. In order to achieve this degree of monitoring, systems are to be put in place and detailed records are also to be kept. These records and processes are (or can be) inspected by the relevant Regulator.

Money laundering techniques and operations can vary in the extreme from the sophisticated use of multiple bank accounts, setting up of businesses, Trusts and the use of nominees and moving criminal proceeds throughout the world, to simply hiding the proceeds of crime under the bed.

Perhaps most commonly the proceeds of crime comes in the form of cash, typically in bank notes, which the criminal must be able to either convert into another form which the criminal can invest or spend without arousing suspicion, or remove it to a safe location, often overseas.

Crimes such as drug trafficking, cigarette smuggling, bootlegging and other acquisitive crime typically generate large sums of cash. This cash is normally in low denomination notes, typically £20 and £10 notes.

This cash is often referred to as "street cash"

A Bank of England banknote weighs approximately 1 gram. Therefore £100,000 in £20 notes weighs approximately 5kgs. This weight of cash would be greater if £10 and £5 notes also made up the £100,000. Furthermore, if the banknotes were old and soiled, the note would weigh more due to the soiling. Accordingly, large amounts of street cash can be bulky and, in the case of drug trafficking for instance, can weigh more and be more bulky than the actual drugs themselves. As an example street cash exchanged for a kilogram of cocaine, sold for £48,000 (made up of £20 banknotes) would weigh approximately 2.4 kgs.

Typically cash is the main medium of exchange that criminals use to trade with each other, as it is readily accepted as payment (although subject to the risk of reporting to the Authorities and unwanted questions being asked), it is largely untraceable and the value is normally well maintained. This cash is often recycled; the cash (for example from the sale of drugs) can be used to pay for the previous shipment (which may have been purchased on credit) or to pay for the next future shipment.

Successful criminals generating large quantities of street cash on a regular basis face a number of problems in disposing of this large quantity of "paper". The safest way is often for the criminal to pass this cash, as quickly as possible, to a trusted individual or organisation that can provide the service of laundering the cash and returning the value to the criminal in a location and form where the criminal can then enjoy the proceeds. Such professional money laundering organised crime enterprises can attract a lot of criminals and criminal monies, until they are disrupted or, for some reason, they fail to deliver.

Money Laundering – Terminology

Despite the simplicity, or complexity of money laundering schemes, most kinds can be roughly divided into three stages, these are commonly referred to as placement, layering and integration.

Placement

The term placement is usually defined as the attempt to put criminally derived funds into the financial system unnoticed.

Large sums of street cash can be generated through crime. However the increased level of anti-money laundering legislation and growing regulation has increased the scrutiny on transactions and, in particular cash transactions, and deposits into the financial sector. An example of placement is where the criminals deposit the street cash into a bank account (or into a number of such bank accounts), by making multiple but small deposits, at a number of different branches, over a period of time in order to minimise scrutiny by the financial institution(s). This method is sometimes known as "smurfing" (or 'structuring').

Layering

This term refers to a series of related transactions intended to further distance the criminal proceeds from their true source, and normally occurs once the proceeds have been placed into the financial sector. This could be through companies, Trusts, informal client accounts etc before being placed into the Regulated Sector.

For example, once criminal proceeds have been deposited with a bank, the proceeds may then be transferred through a number of bank accounts, perhaps in several countries, so making the task of tracing the origin of the funds more difficult.

Integration

This is normally referred to as the last stage of the money laundering process and concerns the removal of the criminal proceeds from the financial system, the proceeds now giving the appearance that these funds have derived from a legitimate source.

The criminal can then enjoy these funds, the proceeds now being laundered. For example, the criminal may receive a banker's draft from a solicitor's client account, giving the appearance of the profits from a property transaction.

Money Laundering Systems

The following model has four key roles.

- Controller A trusted individual (normally based overseas) who arranges the collection of "street cash" in the UK, and who has the ability and means to deliver the proceeds (or value) to a chosen destination.
- Collector An individual who acts on the instructions of the Controller to collect street cash from criminals and dispose of it as directed by the Controller.
- Co-ordinator An intermediary who manages some distinct part of the money laundering process for one or more Controllers.
- Transmitter A person who receives and, by various means, then dispatches money (the street cash) to the (further) control of the Collector.

The Controller is the key to the success of the system. The Controller acts in the same way that the Bankers' Automated Clearing Services (BACS) system operates within mainstream banking in the United Kingdom, balancing credits and debits.

The Controller needs to know where to collect the street cash, how much, and where to send the value. The Controller will typically service a number of criminal organisations. Equally, the criminal (subject to the extent of his relationship and knowledge of professional money launderers) may have access to a number of distinct Controllers, and these Controllers will compete on the various market terms, offering their services in at times a highly competitive market.

The Controller will normally be responsible for the street cash from the moment when it is collected from the criminal, to when it is paid back to the criminal as instructed and after the laundering procedures have been completed. Accordingly, the Controller will 'stand the loss' and be responsible for any cash that is stolen, or seized by the Authorities, and will 'pay out' to the criminal the respective amount regardless. Reputation is highly important, and if for some reason the Controller cannot deliver, the criminal business will move elsewhere. Controllers are usually based abroad, typically in Dubai or Pakistan, but they can, and do also operate elsewhere.

The Controller will typically agree to collect the street cash in the UK and deliver the 'value', or the amount of that street cash to the chosen destination of the criminal or criminal group. Typically the fees charged will be dependant on a number of factors, including the particular client, market forces (both within the legitimate and illegitimate economies), value and risk. These fees may be a percentage, or a certain rate of the monies obtained, but Controllers can equally rely on monies made through managing (and even manipulating) the currency exchange rates, or they will make their profit, more often than not, by both means.

Controllers rely on a Collector, or series of Collectors to physically meet with the criminals, and to then obtain the criminal street cash. Accordingly, the Collectors take the most risk in the laundering enterprise – generally as they are 'hands-on' with large quantities of street cash, and are to personally meet with the criminal.

The Collector is, however, more than a mere courier. The Collector is the trusted representative of the Controller in the UK and can have ties, through family and/or ethnic background, with the Controller. The Controller will know (from the Criminal or Criminal group) how

much street cash is to be collected, from where, when, and usually from whom, although the Criminal's representative's true name may not be given. These necessarily required details will be passed on to the Collector.

The Collector will often then contact the criminal representative with the street cash, and usually arrange a discrete location and an explicit time for the handover to take place. Once the street cash is collected, the Collector usually counts it at a location considered safe by the Collector, whether that be at the Collector's home address, business address, or a "safe house".

Due to the quantities of street cash collected, the Collector often has some type of cash counting machine in order to count the cash. The Collector will also keep a specific record, in some form, to account for how much was collected, from whom, noting any shortages, forgeries or other anomalies, and how the street cash has since been disbursed, as the Collector will have to answer and account to the Controller. Once matters are reconciled to the satisfaction of the Controller, the Collector's records are often subsequently destroyed.

The role of the Collectors has somewhat modified over a period of time as counter measures have been taken by the Controllers to further disguise the origin of the criminal proceeds and the subsequent disposal of the cash. The Controllers may use a Co-ordinator, often based in the UK or Europe, to oversee the activities of the Collectors. These Co-ordinators may act as Collectors, or Transmitters (see below) in their own right. Accordingly, indications of this type of relationship will be shown by instructions being passed through a chain of people.

Once the Collector has the street cash, the Collector must now dispose of the cash, which will be at the direction of the Controller. To the Controller, the sterling cash is merely a commodity which is only of a value if someone else will accept it.

Typically there are four main methods utilised by the Controller to dispose of the cash, namely cash smuggling, money transmission, cash payments and third party deposits.

Cash Smuggling

Smuggling street cash out of the country is one method employed by the Controller. Such street cash can be moved to another country, where it is kept in currency 'cash pools' (an accumulation of bank notes of a particular currency type) for use at a later date. For this to occur, the street cash is smuggled out of the country, perhaps by freight or by courier.

There are not UK currency controls on cash being taken out of the country, however cash to the value of £1,000 or more, and which is suspected of being from crime, or to be used in crime, can be seized by the Authorities; such a seizure is in addition to those persons found to be smuggling the cash now also being liable to arrest. Accordingly, the cash smuggler will often take protective steps to minimise the risk of being caught.

As has been said earlier, £100,000 in £20 banknotes can weigh approximately 5kgs. The Bank of England banknotes have dimensions of 149mm x 80mm x 0.1mm. If new, this quantity of banknotes would be 500mm tall. If the banknotes were well used, this bundle of banknotes would be considerably more bulky.

Accordingly, sterling banknotes can be significantly voluminous, and difficult to conceal

Consequently one method used to reduce the volume of sterling banknotes is to exchange them for large denomination foreign notes. This also assists in concealing/disguising the true origin of the banknotes by changing the form of its value. The highest value sterling banknote in circulation within the UK mainland is the £50 banknote (Scotland do have a £100 note). In the United States, the $100 banknote is the highest denomination, and within the Eurozone, the €500 banknote is the highest denomination note. The Euro also has high denomination notes of €200 and €100. The €500 banknote has dimensions of 160mm x 82mm x 0.12mm and weighs 1.1g (unsoiled). At an exchange rate of £1 to €1.19048 (as of 12th September 2013, 11:20 GMT from www.xe.com), a single €500 banknote is equivalent to £419.998.

£100,000 equivalent of €500 banknotes (238 banknotes) can be carried on the person without arousing suspicion, fitting into a standard size envelope (the bundle weighing 261.8g and being 28.56 mm thick). £25,000 equivalent of €500 banknotes (60 banknotes) can fit in a cigarette packet (the bundle weighing 66g and being 7.2mm thick). Accordingly, the €500 banknote has seemingly become the banknote of choice of criminals.

On 20th April 2010, the wholesale supply of €500 banknotes ceased within the UK. This was as a result of Project Restful (an initiative of the Serious Organised Crime Agency), the aim of which was to deny organised crime access to €500 banknotes.

I have seen that since this time, criminals have moved to the use of the €200 and €100 banknotes, which are still exchanged within the United Kingdom.

Exchange of currency is Regulated and subject to the reporting of Suspicious Activity Reports (SARs) to NCA. Accordingly, money launderers frequently use complicit Bureau, or those with lapse systems and controls to exchange currency.

Cash Payments

The Controller can also dispose of sterling banknotes (the street cash) by passing them on to criminals and other parties who want access to sums of cash (some of which can amount to substantial quantities). Cash, due to its very nature, is almost untraceable and, in itself, can disguise the origins of other criminal proceeds.

For example, a fraud perpetrated against a bank account will leave a chain of transactions which can ultimately be traced. A fraudster stealing £100,000 from a business bank account by falsifying a telegraphic transfer request will receive the £100,000, but it can be found in another bank account (whether or not set up with false details) as identified by the fraudster. The value of the money is still within the financial sector and the fraudster still has the difficulty of accessing these proceeds, before discovery by either the bank or the holder of the defrauded bank account.

One method of obtaining the value of this stolen money would be to use a Controller. The money could be transferred to an account, or accounts of the Controller's choosing anywhere in the world, where those monies may well be further transferred, through several other banks and several other countries, making Law Enforcement's and the bank's task of tracing the flow of the money difficult and slow. In return the Controller could supply cash (as obtained by a Collector, and held in one of the 'cash pools' referred to earlier) to the fraudster.

Accordingly the fraudster now has a medium of exchange which he can spend without directly linking himself to the defrauded account, and the Controller has disposed of some of the cash surplus he has obtained.

On the other hand, a criminal who obtains street cash as a result of his nefarious activities can physically hold on to that cash, and/or hide it away, which makes it more difficult for others to trace.

Money Transmission

A further way that the Controller can dispose of the criminal street cash is by passing that cash to a Transmitter. In my experience, this has tended to be a Money Service Business (MSB), usually run by the same ethnic group as the Controller. The Controller frequently has access to, and uses a number of MSBs, or may use "Agents" to MSBs as a means of dividing up the cash into smaller blocks to send abroad (An MSB Principal / Agent relationship can be said to exist when one entity (the Agent) acts on behalf of another MSB (the Principal)).

Historically, the Controller has made use of complicit MSBs to receive and dispose of the criminal street cash.

In this scenario the Collector takes the street cash to the MSB as directed by the Controller. The Controller will usually have first dealt with the MSB, and agreed the receipt of the cash, negotiated an exchange rate, if appropriate, for the conversion of the sterling to another currency, and given details of which account (usually abroad) and in what currency the value (amount) is to be transferred. The Transmitter/ MSB will pay the street cash into their own account, or sell the cash on to a cash 'wholesaler' and then transmit the agreed amount as directed. The destination account could be one of the Controller's accounts (for example in Dubai, Pakistan or the United States of America), a cash 'pooling account', or a third party account, but it is most likely to be an account ultimately under his control. On receipt of the monies into their account/s, the Controller will be able to use it in order to complete other business transactions (legitimate or otherwise), which assists in 'masking', concealing the true origin of the funds.

Third Party Payment

Approximately ten years ago, disposing of street cash using third party payments became increasingly popular, with money launderers, as a means of disguising the origins of criminal proceeds. Launderers, such as complicit MSB operators, apparently became 'uncomfortable' depositing large sums of criminally derived street cash into their own bank accounts, which then invited increased scrutiny from the Authorities into the origins of the funds and into their "clients" who were depositing the cash.

In addition to customers within the UK, the Controller will probably have clients (legitimate and criminal) in other parts of the world who will (or may) have the need for transactions to be concluded within the UK.

For example, a Pakistani textile manufacturer may be legitimately importing machinery from the UK into Pakistan. Obviously the UK supplier will need to be paid. The Pakistani importer may approach the Controller whom he knows, agree an exchange rate and pass over

the required payment in Pakistani Rupees, or perhaps United States dollars, to that Controller. Controllers are often in a position to offer better exchange rates than commercial or state banks (largely due to lower overheads and operating costs, and the avoidance of legitimate tax implications). The Controller will also be given details of the UK bank account (of the UK supplier) to which the sterling equivalent must be paid. The Controller may then contact his Collector and pass on the relevant bank account details and the amount to be paid. The Collector may then pay the given amount (from the criminally derived street cash he has previously collected and which he still holds) into the given UK supplier's bank account.

It is relatively common for foreign students from the middle-east and the Asian sub-continent, and who are studying in the UK, to receive similar, but smaller payments of value in the same way from friends and relatives who are usually located in the student's home country.

This particular system of "third party payment", can also be known as "cuckoo smurfing". The term "smurfing" generally relates to large sums of criminal street cash being 'broken down' into smaller amounts, and these smaller amounts being deposited into an account, or accounts, over a number of branches, over a time period, with the purpose of disguising the true origin of the cash. The term "cuckoo smurfing" is so called as small sums of criminal cash are deposited in a number of third party accounts, where the account holders may not know the true origin of the cash being deposited, but are expecting, for whatever reason, to receive an amount of money into their bank account.

The term "cuckoo smurfing" has arisen as the process is said to be somewhat similar to the Cuckoo bird laying eggs into the nests of unsuspecting birds, which then raise the cuckoo hatchling as its own.

A Collector involved in Cuckoo smurfing will often receive the details of a number of separate bank accounts together with the various amounts to be paid from the Collector. The Collector, or a series of Collectors working together, may then physically go around a number of different banks and branches paying in the criminal street cash as they have been directed. The Collector engaged in this activity will often visit a number of different branches of the same bank paying in the street cash, rather than paying in a series of transactions for a particular bank account at a single branch, this is to avoid unwanted attention. In this way, a large sum of criminal street cash can be disposed of relatively quickly and comparatively safely.

Once the street cash has been paid into the banking system, the Collector will notify the Controller, and may often prove that the transaction has actually taken place with reference to the paying in slip. This information may be communicated by various means, some prefer simple mobile 'phone text messages ('texting'), others favour transfer of images (photographs) of the paying-in slips being sent by 'phone messaging, but an assortment of means will achieve the desired communiqué. The Collector will also usually record and account for the reduction of the street cash 'stockpile', or 'pooled' monies he has in his control.

Despite the increasing levels of legislation and regulation which have arisen to combat money laundering, one area within banking has remained subject to minimal scrutiny. Unlike any other transaction within the UK banking sector, proof of identity is not necessarily required (as a matter of course) to make deposits into bank accounts. "Cuckoo smurfing" attempts to exploit and take advantage of this fact.

Additionally, the Controller benefits, and therefore profits, from both the receipt of the original criminal street cash and the settlement of the transactions into the UK bank accounts from the businesses or individuals requiring the payments. Controllers will often trade in these third party payments in order to have sufficient transactions to dispose of the entire volume of criminal street cash they have collected and stored within their 'pooling' accounts.

Money Service Businesses

Under the Money Laundering Regulations 2007, a business is described as a Money Service Business (MSB) if it does one or more of the following:

- Acts as a bureau de change
- Transmits money, or any representation of money, in anyway
- Cashes cheques that are payable to customers

This means that any person who, or business which carries out any of the above activities, whether or not for profit, is required to be officially registered and becomes part of the 'Regulated Sector' and subject to all the rules and regulations imposed within the system.

All Money Services Businesses are required to register with HM Revenue & Customs (HMRC). Registration brings with it the following requirements:

- A MSB must carry out Customer Due Diligence which includes identifying customers and the source of funds
- Maintain records of transactions
- Appoint a money laundering reporting officer (MLRO)
- Report suspicious transactions to law enforcement
- Maintain internal systems of training
- Undertake risk assessments, monitoring and control

Furthermore, MSBs engaged in money transmissions must register with the Financial Services Authority (FSA) for the purpose of the Payment Services Regulations 2009. On registration, a MSB will then be afforded the status of:

- Approved Payment Institution, or
- Small Payment Institution (under €3 million turnover per month)

The Payment Services Regulations require periodic reporting to the FSA for the purpose of supervision. The purpose of the Payment Services Regulations is essentially to protect the deposits of monies of customers, rather than any aspect of anti money laundering.

Criminal Exploitation of Money Service Businesses

MSBs are a legal entity within the United Kingdom but need to be officially registered. They can perform an important role for certain sections of the community, for example providing services of money transmission, or value transfer, to other areas of the world where the traditional banking sector is not as prevalent or perhaps ineffective.

However, MSBs have also been illegitimately used extensively by criminals to launder monies. This is due to a number of converging factors including the traditional lack of records (addressed by the Money Laundering Regulations), the lack of reporting to the Authorities (addressed by the Money Laundering Regulations), the minimal risk of losing cash (once

accepted by a MSB, the monies will be paid out) and the ability to pay out monies virtually anywhere in the world, and that being achieved quickly.

Tokens

Ordinarily Collectors have to identify and then meet They may not have to meet (drops etc.) with the criminal or the criminal's representative to collect the street cash to be laundered. The two parties involved may have never met or dealt with each other before, which can cause them some difficulty.

In order to overcome this problem those involved employ the use of 'tokens', used extensively as a means of identifying the Collector to the other criminal, and which can also act as a form of receipt for the street cash collected, the banknote 'token' often being handed over to the criminal (or his associate) at the time of the transaction. The 'token' usually comes in the form of the unique serial number of a particular banknote. The banknote utilised as a token is usually a £5 banknote, but I other denominations and other currencies are used. The banknotes to be used as tokens are provided by the Collector, accordingly the Collector would prefer to hand over a £5 banknote as opposed to a £20 banknote.

Where tokens are used in this manner the Controller will, from time to time, request the token numbers from the Collector. The Collector will then pass over the serial numbers (either the full number or a partial number, usually the first two letters and the last four numerical digits) of banknotes already in his possession (and usually from within the street cash he has already amassed). Once a collection of street cash has been arranged with the Controller, the Controller will then pass a token (the banknote serial number) to his criminal customer. When the criminal (or his representative) meets the Collector, the Collector will then pass over the token (the particular banknote containing the serial number and which has been passed between them), this will be checked by the criminal against the number he has earlier been given by the Controller. Once the criminal is content, the street cash will be handed to the Collector. The criminal may keep the banknote token as proof of the handover.

Scottish and Northern Ireland Banknotes

Often large quantities of Scottish banknotes, and some Northern Ireland banknotes are found in money laundering investigations. This is despite the cases being centred in England. There is not a substantial differnce between levels of crime in England and Scotland, however significant quantities of Scottish currency can be (and often are) found in street cash (£10 and £20 banknotes).

Three banks in Scotland are authorised to issue banknotes. These are Bank of Scotland PLC, Clydesdale Bank PLC and The Royal Bank of Scotland PLC. Four banks in Northern Ireland are authorised to issue banknotes. These are Bank of Ireland (UK) PLC, AIB Group (UK) PLC (which trades as First Trust Bank in Northern Ireland), Northern Bank Limited (which trades as Danske Bank) and Ulster Bank Limited.

Banknotes issued by these banks are "legal currency" Please see below….and can be accepted throughout the United Kingdom. Equally, holders of Scottish and Northern Irish banknotes have the same legal protection as holders or Bank of England banknotes. Scottish and Northern

Irish banknotes are not "legal tender" (this includes in Scotland and Northern Ireland). Indeed Bank of England banknotes are not "legal tender" in Scotland and Northern Ireland. However, in practical terms, "legal tender" does not affect day to day transactions or whether these banknotes can be accepted. Many other transaction methods such as cheques and debit card transactions are also not "legal tender". It is a matter for the two parties involved in the transaction as to what method of payment they are willing to accept

Accordingly, Scottish and Northern Irish banknotes can be accepted, throughout the United Kingdom, however in practise, how readily Scottish and Northern Irish banknotes are accepted throughout the country vary, dependent on a number of factor's including the trader's exposure to the particular banknotes, geographical proximity, particular Scottish / Northern Irish trading patterns, and willingness to trade with them.

Scottish and Northern Irish banknotes are only issued by the respective banks in their particular country (including Automated Teller Machines - ATM). Equally in England and Wales, only sterling banknotes are issued in English banks. Accordingly Scottish and Northern Ireland banknotes received by English banks are repatriated to the issuing banks and are not recycled within the banks (i.e. they do not again become public after the banknotes are received by the bank).

Scottish banknotes are normally not given out to foreign (or overseas) institutions requiring sterling (for example for use in a Bureau de change), the banknotes tend to be Bank of England banknotes. Additionally foreign Bureau de change are reluctant to receive Scottish banknotes. Accordingly, Scottish banknotes are difficult to dispose of abroad, especially in any quantity.

Even within England, although English banks and financial institutions will accept Scottish banknotes, they may be suspicious of the presence of large numbers of these notes in areas where the banknotes are not normally used, or the banknotes' occurrence is not standard for that particular customer of the bank.

This causes a problem to criminals who may have conducted a transaction with their associates located in Scotland or Northern Ireland and, as a result, taken possession of such banknotes as payment; accordingly, Scottish and Northern Irish banknotes tend to be 're-cycled' between criminals in transactions. Over time, the volume of Scottish and Northern Ireland banknotes can grow within the cash reserves of the criminal groups, who cannot readily dispose of these notes without difficulty or arousing suspicion.

Money laundering organisations operating within England and Europe face the same problems with the Scottish and Northern Ireland banknotes and have been known to charge a premium (simply a higher than normal amount being charged) to deal with these notes.

Communications

Effective communications are essential for a money laundering organisation to operate. The use of telephones, facsimile and computers are used to pass on information, as well as face to face meetings and the passing of documents. In the laundering systems explained above, communications are very important in putting parties (who may not know each other) together. As has been explained, the Controller is key to the laundering system, and it is equally the Controller who is at the centre of communications. There will need

to be communication between the criminal requiring the money laundering service and the Controller or a Co-ordinator. The "deal" needs to be arranged. The Controller/ Co-ordinator needs to know how much is to be laundered, where the cash is to be collected/ delivered and importantly the fee for that particular transaction needs to be negotiated and agreed. Once this "deal" has been agreed, the Controller must contact his associates and the criminal will contact his representatives.

If tokens are to be used, the Controller will need to seek and then receive token numbers from the Collector. Then the unique token number will have to be passed to the criminal who, in turn, may pass this to his representative delivering the street cash. The Collector will then need to notify the Collector of where they have to travel to collect the cash (though this can also be arranged direct between the criminal and the Collector, and may, over time as regular transactions are completed, become a repetitive meeting place), when this is to take place, a means of contacting the criminal group, and confirmation of the token number to be used. After the collection has been made and the street cash counted, the Collector will have to confirm the count to the Controller. The Controller will then need to inform the Collector on how he is to dispose of the street cash.

This is usually done by telephone and frequently text messages are passed, especially with specific details such as postcodes (to identify the location of the meet – for which SatNavs, or some means of global positioning system are frequently used by Collectors to identify locations), token numbers, contact telephone numbers and amounts.

Brian Ludlow
Economic Crime Command, National Crime Agency, UK

Pranie brudnych pieniędzy w obrocie handlowym (TBML)

Streszczenie

Pranie brudnych pieniędzy w obrocie handlowym (TBML) jest prawdopodobnie najbardziej rozpowszechnioną obecnie formą prania pieniędzy, potencjalnie przenoszącą największą część dochodów pochodzących z przestępstw na całym świecie. Co niepokojące, najprawdopodobniej jest to również forma prania brudnych pieniędzy, która jest w najmniejszym stopniu badana lub wręcz unikana przez organy ścigania. Jaki jest powód takiej sytuacji? Prowadzenie śledztwa w takich sprawach może być trudne i czasochłonne. W związku z tym przez system handlowy przepływają miliardy dolarów pochodzących z działalności przestępczej. TBML to wykorzystywanie handlu w celu ukrycia przepływu dochodów pochodzących z działalności przestępczej. Pieniądze przestępców giną dzięki temu w 'białym szumie" generowanym przez miliony transakcji handlowych przeprowadzane na całym świecie. TBML pozwala na przenoszenie wartości bez fizycznego przekazania pieniędzy; niszczy ścieżki audytu; ukrywa własność faktyczną; może ułatwiać dokonywanie innych przestępstw, na przykład unikania opodatkowania i zasad dotyczących walut. TBML może przybierać wiele form i odmian. Niniejsza prezentacja ma na celu wyjaśnienie niektórych aspektów TBML, cech tego procederu i sposobu rozpoznawania. Co ważne, prezentacja dąży do wypracowania metod walki z tym problemem.

Pojęcie „prania brudnych pieniędzy" jest bardzo często rozumiane w znaczeniu działań podejmowanych przez przestępców lub zorganizowane grupy przestępcze, mających na celu uwiarygodnienie źródła pochodzenia pieniędzy zdobytych w wyniku działań przestępczych, aby umożliwić ich wykorzystanie bez ryzyka wykrycia lub zatrzymania. W praktyce znaczenie tego terminu jest jednak dużo szersze.

Często uznaje się, że większość przestępstw jest popełnianych w celu uzyskania korzyści finansowych. W związku z tym przestępczość motywowana finansowo (jeśli zakończy się sukcesem) będzie generować dochody (określane technicznym mianem „korzyści pochodzących z przestępstwa"). Korzyści pochodzące z przestępstwa mogą stanowić wyłącznie gotówkę, jednak w niektórych przypadkach mogą obejmować także majątek uzyskany w wyniku czynu przestępczego. Wszelkie działania polegające na uzyskiwaniu, posiadaniu, ukrywaniu lub wykorzystywaniu w jakikolwiek inny sposób korzyści pochodzących z przestępstwa określa się mianem prania brudnych pieniędzy. Ta niezwykle popularna definicja jest wielokrotnie przywoływania w ustawodawstwie i systemach regulacji podatkowych, a także w środowisku akademickim.

Ogólnie rzecz ujmując, jednym z pierwszych zadań przestępcy uzyskującego korzyści z przestępstwa jest upewnienie się, że można z nich bezpiecznie korzystać. Przestępca chce zwykle mieć możliwość korzystania z uzyskanych środków bez wzbudzania podejrzeń władz lub innych osób, które mogą powiadomić władze, co może w konsekwencji doprowadzić do aresztowania oraz przepadku mienia. W związku z tym przestępca rozpocznie proces „prania" uzyskanych korzyści, aby móc bez obaw z nich korzystać.

W Wielkiej Brytanii pranie brudnych pieniędzy zostało uznane za przestępstwo na mocy przepisów uchwalanych przez Parlament. Działania w zakresie prania brudnych pieniędzy obejmują między innymi:

- ukrywanie, przekształcanie, przenoszenie mienia przestępczego,
- wywożenie mienia przestępczego z danej jurysdykcji,
- zawieranie umów mających na celu ułatwienie zdobycia mienia,
- przechowywanie, korzystanie lub posiadanie mienia pochodzącego z przestępstwa – w tym wypadku należy zachować ostrożność, aby nie uzurpować sobie roli sędziego bądź musieć odpowiadać na pytania związane z samym prawem w oderwaniu od kontekstu.

Poszczególne sektory i branże narażone na wykorzystywanie przez przestępców zajmujących się praniem brudnych pieniędzy zostały objęte odpowiednimi regulacjami, nastąpiła także ich rejestracja.

Przedsiębiorstwa należące do tak zwanego „Sektora regulowanego" (pojęcie wymaga dodatkowego objaśnienia dla osób niezwiązanych z tematem) są zobowiązane do uzyskiwania informacji dotyczących transakcji od swoich klientów, a także sprawdzania poszczególnych transakcji w celu upewnienia się, że nie zachodzi podejrzenie prania brudnych pieniędzy oraz zgłaszania podejrzanych transakcji – podejrzenia tego typu są zgłaszane do NCA (National Crime Agency – brytyjska agencja rządowa zajmująca się walką z przestępczością, przyp. tłum.) W celu osiągnięcia takiego stopnia monitorowania wymagane jest stworzenie odpowiednich systemów i sporządzanie szczegółowej dokumentacji. Tego rodzaju dokumentacja i procesy są (lub mogą być) badane przez odpowiednie organy administracji.

Techniki prania brudnych pieniędzy i związana z tym procederem działalność przestępcza może opierać się na wielu schematach, od wykorzystania wielu kont bankowych i zakładania firm, spółek i funduszy powierniczych, a także przenoszenia korzyści pochodzących z przestępstwa po całym świecie, może także polegać wyłącznie na ukryciu zdobytego nielegalnie majątku pod łóżkiem.

Najpopularniejszym i najczęściej występującym rodzajem korzyści pochodzących z przestępstwa jest gotówka, zwykle w formie banknotów, którą przestępca musi przekształcić w inny środek płatniczy możliwy do zainwestowania lub wydania w sposób niewzbudzający podejrzeń lub przeniesienia go w celu ukrycia w bezpiecznym miejscu, często za granicą.

Przestępstwa takie jak na przykład przemyt narkotyków oraz papierosów, fałszerstwa lub inne występki polegające na pozbawieniu własności zazwyczaj generują duże ilości gotówki. Gotówka ta stanowi zazwyczaj duże liczby banknotów o niskim nominale, zwykle 10- i 20-funtowych, często określanych mianem „pieniędzy ulicznych".

Banknot wydany przez Bank of England waży około 1 grama. Na tej podstawie łatwo obliczyć, że 100 000 funtów w banknotach 20-funtowych waży około 5 kilogramów. Oczywiście,

waga ta wzrośnie w sytuacji, gdy w kwocie tej znajdą się także banknoty 5- i 10-funtowe. Co więcej, jeśli banknoty są starsze i zabrudzone, ich waga będzie nieco większa. W związku z tym duże ilości gotówki mogą być nieporęczne. W przypadku wielu rodzajów przestępstw takich jak przemyt narkotyków pieniądze mogą ważyć więcej i zajmować więcej miejsca niż same narkotyki. Dla przykładu, gotówka otrzymana w zamian za kilogram kokainy warty 48 000 funtów (w banknotach 20-funtowych) będzie ważyła w przybliżeniu 2,4 kilograma.

Zwykle to gotówka stanowi główny środek wymiany i handlu dla przestępców, ponieważ jest bezproblemowo przyjmowana jako środek płatniczy. Korzystanie z niej wiąże się jednak z ryzykiem zgłoszenia do odpowiednich organów oraz konieczności udzielania odpowiedzi na niewygodne pytania. Co więcej, przepływ gotówki jest niezwykle trudny do prześledzenia, a dodatkowo jej wartość pozostaje zwykle w dużej mierze niezmienna. Tego typu pieniądze często zmieniają właścicieli – gotówka (pochodząca z przykładowej sprzedaży narkotyków) może zostać wykorzystana w celu zapłacenia za poprzednią dostawę, która mogła zostać zakupiona „na kredyt", lub w celu zapłaty za kolejne dostawy.

Skuteczni przestępcy, którym regularnie udaje się zdobywać duże ilości drobnych banknotów mają do czynienia z wieloma problemami związanymi z pozbywaniem się takich ilości papierowych pieniędzy. Najskuteczniejszym i najbardziej bezpiecznym sposobem rozwiązania problemu jest przekazanie tych pieniędzy – tak szybko jak to możliwe – zaufanej osobie lub organizacji, która jest w stanie zapewnić usługę prania brudnych pieniędzy i przekazania korzyści z przestępstwa do wybranego miejsca w formie, która pozwoli przestępcy skorzystać ze zdobytych środków. Tego rodzaju organizacje przestępcze zajmujące się praniem brudnych pieniędzy mogą przyciągać wielu kryminalistów i środków pochodzących z przestępstw do czasu, w którym ich działalność zostanie zakłócona lub z jakiegoś powodu nie będą mogły zrealizować usługi.

Pranie brudnych pieniędzy – terminologia

Pomimo faktu, że działalność polegająca na praniu brudnych pieniędzy może być niezwykle prosta lub złożona, większość tego typu działań można podzielić na trzy główne etapy, które można określić mianami „umiejscowienia", „maskowania" oraz „legitymizacji".

Umiejscowienie

Termin ten definiowany jest zazwyczaj jako próba niepostrzeżonego umieszczenia korzyści uzyskanych w wyniku przestępstwa w systemie finansowym.

Działania przestępcze mogą prowadzić do uzyskania dużych ilości gotówki. Jednakże stale zwiększająca się liczba praw i regulacji mających na celu przeciwdziałanie procederowi prania brudnych pieniędzy doprowadziła do zwiększenia kontroli transakcji, w szczególności transakcji gotówkowych oraz wpłat. Przykładem umiejscowienia jest próba wpłaty przez przestępcę zdobytej gotówki na konto bankowe (lub wiele kont bankowych) poprzez dokonywanie wielu mniejszych, rozłożonych w czasie wpłat w wielu oddziałach w celu uniknięcia kontroli ze strony instytucji finansowych. Metoda ta jest znana także pod nazwą „smurfingu" lub „structuringu" – rozbijania wpłat.

Maskowanie

Termin ten określa dokonywanie wielokrotnych, połączonych ze sobą transakcji, mających na celu oddalenie środków pochodzących z działalności kryminalnej od ich źródła. Zwykle dochodzi do niego po umieszczeniu środków w systemie finansowym. Tego typu działalność może odbywać się przy pomocy firm, spółek, innych kont itd. przed umieszczeniem środków w sektorze regulowanym.

Na przykład po umieszczeniu korzyści pochodzących z przestępstwa na kocie bankowym, pieniądze mogą zostać przesłane przez wiele kont znajdujących się w kilku krajach, dzięki czemu zadanie prześledzenia miejsca pochodzenia środków stanie się znacznie trudniejsze.

Legitymizacja

Etap ten jest zwykle określany mianem ostatniego etapu w procesie prania brudnych pieniędzy i wiąże się z usunięciem środków z systemu finansowego.

Na tym etapie środki zdają się pochodzić z legalnego źródła. Na przykład przestępca może otrzymać czek z konta klienta kancelarii prawniczej, sprawiając tym samym wrażenie, że dochody pochodzą ze sprzedaży nieruchomości.

Systemy prania brudnych pieniędzy

Przedstawiony przykład systemu prania brudnych pieniędzy obejmuje cztery główne role:

- **kontroler** – zaufana osoba, zwykle przebywająca za granicą, organizująca odbiór gotówki na terenie wielkiej brytanii. zwykle osoba ta ma możliwość dostarczenia pieniędzy pochodzących z przestępstwa do wybranego miejsca,
- **odbiorca** – osoba działająca na podstawie instrukcji przekazanych przez kontrolera w celu odbioru gotówki od przestępców i dostarczenia jej zgodnie z instrukcją,
- **koordynator** – pośrednik, który kieruje jedną z części procesu prania brudnych pieniędzy w imieniu jednego lub kilku kontrolerów,
- **przekazujący** – osoba, która otrzymuje, a następnie na różne sposoby przekazuje gotówkę pod kontrolę kontrolera.

Kontroler pełni w tym wypadku kluczową rolę dla sukcesu całego systemu. W przypadku tego modelu, kontroler działa w taki sam sposób, jak system BACS (Bankers' Automated Clearing Services – system rozliczeń transakcji finansowych działający w Wielkiej Brytanii – przyp. tłum.) działający w głównych brytyjskich bankach, rozliczający poszczególne wpłaty i wypłaty.

Kontroler musi wiedzieć, gdzie należy zebrać gotówkę, jakiej kwoty dotyczy transakcja, a także komu i w jaki sposób przekazać środki. Jeden kontroler zwykle świadczy swoje usługi wielu organizacjom przestępczym.

Przestępcy zaś, w zależności od swoich relacji oraz wiedzy na temat profesjonalnych pralni brudnych pieniędzy, mogą mieć dostęp do wielu kontrolerów, którzy oferują swoje usługi, konkurując między sobą na czarnym rynku.

Kontroler najczęściej ponosi odpowiedzialność za gotówkę od chwili jej odebrania od przestępcy, aż do chwili, w której zostanie przekazana przestępcy zgodnie z instrukcją po zakończeniu procesu prania brudnych pieniędzy. Co więcej, kontroler ponosi odpowiedzialność za wszelkie straty, a także kradzieże lub przepadek pieniędzy na rzecz organów

ścigania i niezależnie od okoliczności jest zobowiązany do wypłaty odpowiedniej kwoty przestępcy. Reputacja jest niezwykle ważna – jeśli z jakiegokolwiek powodu kontroler nie będzie w stanie zrealizować usługi, organizacja przestępcza skieruje swoje kroki do innej osoby. Kontrolerzy zwykle przebywają za granicą, zwykle w miejscach takich jak Dubaj lub Pakistan, jednak często działają także w innych krajach na całym świecie.

Zazwyczaj kontrolerzy zgadzają się na odbiór gotówki w Wielkiej Brytanii i dostarczenie „wartości" lub określonej ilości gotówki do miejsca wybranego przez przestępcę lub zorganizowaną grupę przestępczą. Typowe opłaty za pranie brudnych pieniędzy zależą od wielu czynników, w tym tożsamości danego klienta, uwarunkowań rynkowych (zarówno na legalnym, jak również na czarnym rynku), a także wartości i ryzyka. Opłaty te mogą stanowić odsetek pranych pieniędzy lub określoną kwotę, jednak kontrolerzy mogą w równym stopniu polegać na funduszach zdobytych za pomocą handlu (czasem nawet manipulacji) kursami walut. Często zdarza się, że ich przychód jest generowany jednocześnie z obu źródeł.

Kontrolerzy polegają na usługach odbiorcy lub kilku odbiorców, którzy spotykają się z kryminalistami i uzyskują w ten sposób pieniądze pochodzące z działalności przestępczej. Odbiorcy ponoszą tym samym największe ryzyko w przemyśle prania brudnych pieniędzy z racji tego, że mają osobisty kontakt z dużymi ilościami gotówki i regularnie stykają się z przedstawicielami przestępczego półświatka.

Mylą się jednak ci, którzy uważają, że odbiorca jest wyłącznie posłańcem lub kurierem. W rzeczywistości odbiorca jest zaufanym przedstawicielem kontrolera w Wielkiej Brytanii i najczęściej ma z nim powiązania rodzinne lub etniczne. Kontroler uzyskuje informacje (od przestępcy lub organizacji przestępczej) na temat tego, jak wiele gotówki należy odebrać, gdzie i kiedy nastąpi jej przekazanie, często ustalając także przy tym tożsamość osoby przekazującej, jednak w wielu przypadkach prawdziwe imię i nazwisko przestępcy bądź przedstawiciela organizacji pozostanie nieznane. Wszystkie te przydatne dane i informacje trafiają następnie do odbiorcy.

Odbiorca nawiązuje następnie kontakt z osobą posiadającą gotówkę, a później ustali czas przekazania pieniędzy i wybierze dyskretne miejsce, w którym może dojść do przekazania. Po zakończeniu przekazania odbiorca zwykle przechowuje gotówkę w miejscu uznanym przez niego samego jako bezpieczne – w domu, w firmie lub w kryjówce.

Z racji ilości odbieranej gotówki odbiorca bardzo często posiada maszynkę do liczenia pieniędzy, którą wykorzystuje do przeliczania banknotów, prowadzi także szczegółową dokumentację w dowolnej formie, w której znajdują się informacje na temat ilości i źródła odebranych pieniędzy, wszelkich braków lub wykrytych podróbek, a także ilości wypłaconych dotychczas pieniędzy. Dzieje się tak, ponieważ odbiorca odpowiada i rozlicza się przed kontrolerem. Po zakończeniu transakcji w sposób zadowalający kontrolera, dokumentacja odbiorcy najczęściej ulega zniszczeniu.

Rola, którą pełnią odbiorcy uległa znaczącym zmianom w ramach środków zapobiegawczych podejmowanych przez kontrolerów, mających na celu ukrycie źródła pochodzenia środków pochodzących z przestępstwa, a także dalszych dyspozycji dotyczących pieniędzy. Kontrolerzy mogą korzystać z usług koordynatorów, którzy często przebywają w Wielkiej Brytanii lub w krajach Europy – ich zadaniem jest obserwacja i nadzór nad działaniami

odbiorców. Koordynatorzy mogą także działać w roli odbiorców lub przekazujących (patrz niżej). Informacje dotyczące tego rodzaju relacji wynikają z instrukcji i informacji przekazywanych przez wiele osób.

Po odebraniu przez odbiorcę gotówki konieczne jest jej rozdysponowanie zgodnie z instrukcjami przekazanymi przez kontrolera. Dla kontrolera gotówka stanowi wyłącznie towar, który ma jakąkolwiek wartość tylko wtedy, gdy ktokolwiek zgodzi się ja przyjąć.

Zwykle kontrolerzy stosują cztery główne metody pozbywania się gotówki, są to: przemyt gotówki, transfery środków pieniężnych, wypłaty gotówkowe oraz płatności dokonywane przez osoby trzecie.

Przemyt pieniędzy

Przemyt gotówki poza granice kraju jest jednym ze sposobów wykorzystywanych przez kontrolerów. Zebrana gotówka może zostać przerzucona przez granice do innych krajów, gdzie jest przechowywana w formie pul walutowych (dużej ilości gotówki w wybranej walucie) w celu jej wykorzystania w późniejszym czasie. Aby było to możliwe, gotówka musi zostać w pierwszej kolejności przemycona z kraju, na przykład przy pomocy transportu lub kuriera.

Nie istnieją żadne sposoby kontroli gotówki wywożonej poza terytorium Wielkiej Brytanii, jednak mimo to wszelkie ilości gotówki przekraczające 1000 funtów szterlingów, co do których istnieją podejrzenia dotyczące ich pochodzenia z działalności przestępczej lub możliwości ich wykorzystania do celów działalności przestępczej mogą zostać przejęte przez odpowiednie służby, a osoby podejrzewane o przemyt gotówki mogą zostać aresztowane. Z tego powodu przemytnicy pieniędzy bardzo często podejmują odpowiednie kroki w celu zminimalizowania ryzyka aresztowania.

Jak wspomniano wcześniej 100 000 funtów szterlingów w banknotach 20-funtowych waży około 5 kilogramów. Wymiary standardowego banknotu wydanego przez Bank of England wynoszą 149 x 80 x 0,1 mm. W przypadku nowych banknotów wysokość takiego stosu wynosi 500 milimetrów. W przypadku, gdy banknoty były już używane, ich objętość znacząco rośnie. Co więcej, banknoty brytyjskie są bardzo obszerne i trudne do ukrycia.

W związku z tym jedną z najczęściej wykorzystywanych metod mających na celu zmniejszenie objętości gotówki jest ich wymiana na zagraniczne banknoty w dużych nominałach. Tego typu działanie pozwala także na lepsze ukrycie prawdziwego pochodzenia pieniędzy poprzez zmianę waluty. Największym nominałem funta szterlinga pozostającym w obiegu w Wielkiej Brytanii jest banknot 50-funtowy (w Szkocji dostępne są także banknoty 100-funtowe). W Stanach Zjednoczonych największym nominałem jest banknot studolarowy, podczas gdy w strefie euro dostępne są banknoty o nominale 500 euro, a także 200 i 100 euro. Banknot o nominale 500 euro ma wymiary 160 x 82 x 0,12 mm i waży 1,1 grama (bez zabrudzeń). Biorąc pod uwagę kurs wymiany wynoszący 1 GBP = 1,19048 EUR (z dnia 12 września 2013 roku o godzinie 11:20 GMT, w oparciu o dane ze strony www.xe.com), pojedynczy banknot o nominale 500 euro odpowiada kwocie 419,998 funtów.

Tym sposobem równowartość 100 000 funtów w banknotach o nominale 500 euro (238 banknotów) może być przenoszona bez żadnych podejrzeń przez dowolną osobę, ponieważ mieści się w standardowej kopercie – całość waży 261,8 grama i ma grubość 28,56 mm.

Równowartość 25 000 funtów szterlingów w banknotach 500€ zmieści się do paczki po papierosach (całość będzie ważyła 66 gramów, grubość pakietu wyniesie 7,2 mm). Z tego powodu banknot o nominale 500 euro stał się ulubionym banknotem świata przestępczego.

20 kwietnia 2010 roku zakończyły się hurtowe dostawy banknotów o nominale 500 euro w Wielkiej Brytanii. Stało się tak w wyniku inicjatywy Project Restful zapoczątkowanej przez Serious Organised Criume Agency (Agencję ds. Zwalczania Poważnej Przestępczości Zorganizowanej – przyp. tłum), której celem było odcięcie przestępczemu półświatkowi dostępu do banknotów 500€.

Od tamtej pory przestępcy zaczęli korzystać z banknotów o nominałach 200 i 100 euro, które w dalszym ciągu podlegają wymianie na terenie Wielkiej Brytanii.

Wymiana walut stanowi część tak zwanego Sektora Regulowanego i podlega obowiązkowi przekazywania raportów dotyczących podejrzanych transakcji (Suspicious Activity Reports, SAR) do NCA. Wielu przestępców korzysta z tego powodu z kantorów powiązanych z działalnością przestępczą, a także kantorów z nieszczelnymi systemami kontroli do wymiany walut.

Płatności gotówkowe

Kontroler może także pozbyć się gotówki ulicznej w brytyjskiej walucie poprzez przekazywanie jej innym przestępcom, którzy potrzebują dostępu do gotówki – czasem mogą to być naprawdę duże sumy. Z racji swojego charakteru przepływy gotówkowe są niemal niemożliwe do wyśledzenia i dzięki temu możliwe jest ukrycie źródeł pochodzenia innych środków uzyskanych w wyniku przestępstwa.

Przykładowo, oszustwo bankowe doprowadzi do pozostawienia łańcucha transakcji, który będzie można sprawdzić i prześledzić. Oszust wykradający 100 000 funtów z konta firmowego w banku przez sfałszowanie zlecenia przelewu otrzyma co prawda pieniądze, ale mogą one zostać znalezione na innym koncie bankowym, niezależnie od tego, czy zostało założone na prawdziwe dane osobowe. Wartość ukradzionych pieniędzy pozostaje cały czas w ramach systemu finansowego, a oszust cały czas musi borykać się z trudnościami w dostępie do funduszy aż do momentu wykrycia oszustwa przez bank lub posiadacza konta, wobec którego zostało dokonane oszustwo.

Jednym ze sposobów pozwalających na uzyskanie wartości z funduszy uzyskanych w wyniku oszustwa jest skorzystanie z usług kontrolera. W pierwszej kolejności pieniądze mogą zostać przelane na konto lub konta kontrolera założone w dowolnym miejscu na świecie, następnie zostaną wykonane kolejne przelewy przez inne banki znajdujące się w wielu państwach, co znacząco utrudni i spowolni proces śledzenia przepływów pieniężnych przez organy ścigania i bank. W zamian kontroler może przekazać oszustowi gotówkę (odebraną uprzednio przez odbiorcę i przechowywaną w jednej ze wspomnianych pul). W ten sposób oszust otrzymuje środek płatniczy, który może wydawać bez ryzyka, że zostanie to bezpośrednio połączone z oszustwem bankowym, a kontroler pozbywa się części zgromadzonej gotówki.

Z drugiej strony przestępca, który zdobywa gotówkę w wyniku własnej działalności przestępczej może zdecydować się na jej zatrzymanie i ukrycie, co znacząco utrudni innym prześledzenie jej przepływu.

Transfery środków pieniężnych

Kolejnym sposobem, dzięki któremu kontroler może pozbyć się gotówki pochodzącej z przestępstwa jest przekazanie jej przekazującemu. Z mojego doświadczenia wynika, że najczęściej są to przedsiębiorstwa świadczące usługi w zakresie zarządzania pieniędzmi, zwykle obsługiwane przez grupę etniczna, do której należy także kontroler. Często kontroler ma dostęp do wielu takich przedsiębiorstw, może także wykorzystywać „przedstawicieli" w poszczególnych przedsiębiorstwach w celu podziału gotówki na mniejsze ilości i przesłanie jej za granicę. W przypadku, w którym jeden podmiot (przedstawiciel) działa w imieniu innego podmiotu (zleceniodawcy) mówimy o zależności przedstawiciel-zleceniodawca.

Dotychczas kontrolerzy wykorzystywali powiązane z nimi podmioty w celu odbioru i pozbywania się pieniędzy pochodzących z przestępstwa.

W takim przypadku odbiorca po odebraniu gotówki kierował się do wybranego podmiotu, zgodnie ze wskazaniami kontrolera. Zwykle kontroler wcześniej nawiązywał kontakt z podmiotem i ustalał odbiór gotówki lub negocjował kurs wymiany, jeśli zachodziła potrzeba wymiany funta szterlinga na inną walutę, a także przekazywał informacje dotyczące numeru konta (zazwyczaj zagranicznego) oraz waluty i kwoty pieniędzy, które powinny zostać przelane.

W następnej kolejności przekazujący wpłaca przyjęte pieniądze na swoje własne konto lub sprzedaje pieniądze „hurtownikowi", a następnie przelewa ustaloną wcześniej kwotę. Kontem docelowym może być jedno z kont należących do kontrolera (na przykład zlokalizowane w Dubaju, Pakistanie lub Stanach Zjednoczonych), konto przeznaczone do zbierania środków pieniężnych lub konto osoby trzeciej – najczęściej jednak jest to konto kontrolowane osobiście przez kontrolera. Po wpłynięciu pieniędzy na konto lub konta, kontroler będzie miał możliwość użyć ich w celu przeprowadzenia transakcji biznesowych (legalnych lub przestępczych), co pomoże w dalszym maskowaniu i ukrywaniu prawdziwego pochodzenia środków.

Płatności dokonywane przez osoby trzecie

Około 10 lat temu znacząco wzrosła popularność ukrywania przez przestępców źródeł pochodzenia pieniędzy za pomocą płatności dokonywanych przez osoby trzecie. Pralnie brudnych pieniędzy, na przykład podmioty finansowe powiązane ze światkiem przestępczym zaczęły niechętnie patrzeć na przelewy dużych sum pieniędzy pochodzących z przestępstw na własne konta bankowe, ponieważ powodowało to zwiększenie zainteresowania służb, a w rezultacie dochodzenia dotyczące pochodzenia środków i klientów, którzy wpłacali pieniądze.

Poza klientami przebywającymi na terenie Wielkiej Brytanii, kontrolerzy zazwyczaj znają także klientów (zarówno legalne podmioty, jak i organizacje przestępcze) na całym świecie, którzy mogą chcieć zrealizować transakcje na terenie Wielkiej Brytanii.

Na przykład pakistański producent tekstyliów może legalnie importować maszyny produkcyjne z Wielkiej Brytanii do Pakistanu. W tej sytuacji zachodzi oczywiście konieczność zapłacenia dostawcy z Wielkiej Brytanii. Pakistański importer może w takiej sytuacji skierować swoje kroki do znajomego kontrolera, ustalić kurs wymiany i przekazać mu pieniądze na zapłatę w pakistańskich rupiach lub innej walucie, na przykład dolarach amerykańskich. Kontrolerzy są bardzo często w stanie zaoferować swoim klientom dużo bardziej korzystny kurs wymiany niż banki komercyjne i centralne dzięki niższym kosztom prowadzenia działalności

oraz unikaniu opodatkowania. Kontroler otrzymuje także dane brytyjskiego konta bankowego (należącego do dostawcy w Wielkiej Brytanii), na które powinna zostać wpłacona należność w funtach. Następnie kontroler może skontaktować się ze swoim odbiorcą w celu przekazania odpowiednich danych konta bankowego i kwoty, którą należy zapłacić. Po uzyskaniu wszystkich informacji odbiorca wpłaca podaną kwotę (korzystając z odebranej gotówki pochodzącej z przestępstw, którą ciągle posiada) na konto bankowe brytyjskiego dostawcy.

Odbieranie podobnych wpłat od znajomych, przyjaciół i rodzin przebywających za granicą jest typowe w przypadku studentów pochodzących z Bliskiego Wschodu oraz z krajów azjatyckich – w takiej sytuacji mamy jednak do czynienia z mniejszymi kwotami.

Tego rodzaju system płatności dokonywanych przez osoby trzecie określa się czasem pojęciem „cuckoo smurfing". Termin „smurfing" oznacza przede wszystkim rozdrabnianie dużych sum gotówki na mniejsze kwoty, które są następnie wpłacane przez podstawione osoby („słupy") na jedno lub więcej kont bankowych w wielu oddziałach w dłuższym okresie czasu. Celem procederu jest oczywiście zamaskowanie prawdziwego źródła pochodzenia pieniędzy. Termin „cuckoo smurfing" odnosi się zaś do wpłacania niewielkich sum pieniędzy pochodzących z przestępstwa na konta należące do osób trzecich, których posiadacze nie są świadomi prawdziwego pochodzenia przelewanych pieniędzy, jednak spodziewają się otrzymania pieniędzy na swoje konta bankowe.

Pojęcie to wynika z tego, że opisany proces jest w pewnym stopniu podobny do zachowania kukułki, która składa jaja w gniazdach niczego niepodejrzewających ptaków, które następnie wychowują pisklęta jak własne potomstwo.

Odbiorca, który uczestniczy w procesie „cuckoo smurfingu" często otrzymuje listę różnych numerów kont wraz z listą wpłat, które powinny zostać wykonane. odbiorca bądź kilku współpracujących ze sobą odbiorców, udaje się następnie do kilku różnych banków i oddziałów i dokonują wpłat gotówki pochodzącej z przestępstwa na podane konta. Odbiorca uczestniczący w tym procederze najczęściej odwiedza w tym celu kilka różnych oddziałów tego samego banku wpłacając gotówkę zamiast wykonać serię transakcji związanych z danym kontem bankowym w jednym oddziale, aby uniknąć niepotrzebnego zainteresowania pracowników banku. Ten sposób pozwala na szybkie i – co najważniejsze – bezpieczne pozbycie się dużych ilości gotówki pochodzącej z działalności przestępczej.

Po wpłaceniu pieniędzy do systemu bankowego, odbiorca kontaktuje się w kontrolerem. Często na tym etapie odbiorca musi potwierdzić, że dana transakcja faktycznie miała miejsce przesyłając potwierdzenie wpłaty. Tego rodzaju informacja może zostać przekazana na kilka różnych sposobów – niektórzy wykorzystują potwierdzenia SMS-owe, inni wybierają przesyłanie fotografii potwierdzeń na telefony komórkowe. Słowem, istnieje wiele sposobów przekazywania informacji. Odbiorca następnie dokumentuje i księguje zmniejszenie ilości posiadanej gotówki.

Pomimo coraz ostrzejszych regulacji i praw, które zostały wprowadzone w celu walki z praniem brudnych pieniędzy, jeden obszar bankowości pozostaje pod minimalnym nadzorem i kontrolą. W przeciwieństwie do wszystkich innych transakcji finansowych w sektorze bankowości w Wielkiej Brytanii, dowód tożsamości nie jest z zasady wymagany przy dokonywaniu wpłat na konta bankowe. Proceder „cuckoo smurfingu" stara się wykorzystywać tę lukę istniejącą w systemie kontroli transakcji.

Co więcej, kontroler zyskuje zarówno na odbiorze gotówki pochodzącej z przestępstwa, jak również z rozliczania transakcji na brytyjskich kontach bankowych należących do podmiotów i osób wymagających płatności. Bardzo często zdarza się, że kontrolerzy handlują wpłatami osób trzecich, aby zebrać wystarczającą liczbę transakcji pozwalającą na pozbycie się całości gotówki zebranej w wyniku przestępstw i zgromadzonej na kontach bankowych.

Przedsiębiorstwa świadczące usługi w zakresie zarządzania pieniędzmi

Na mocy ustawy Money Laundering Regulations z 2007 roku (ustawy ds. regulacji związanych z praniem brudnych pieniędzy – przyp. tłum.) przedsiębiorstwo jest określane mianem przedsiębiorstwa świadczącego usługi w zakresie zarządzania pieniędzmi (Money Service Business, MSB) jeśli spełnia jeden z poniższych warunków:

- działa jako kantor,
- przekazuje w jakikolwiek sposób pieniądze lub jakiekolwiek formy pieniędzy,
- wypłacają czeki wystawione na rzecz klientów.

Oznacza to, że każda osoba oraz każdy podmiot, który w ramach swojej działalności wykonuje jedną z powyższych czynności musi zostać oficjalnie zarejestrowany i staje się tym samym częścią Sektora Regulowanego, podlegając zasadom i regulacjom obejmującym cały system, niezależnie od tego, czy działalność ta przynosi dochody.

Wszystkie przedsiębiorstwa świadczące usługi w zakresie zarządzania pieniędzmi podlegają rejestracji w Urzędzie Podatkowym i Celnym Jej Królewskiej Mości (HM Revenue & Customs, HMRC). Rejestracja wiąże się z następującymi wymaganiami:

- podmiot musi dochować należytej staranności w kontaktach z klientami, oznacza to między innymi konieczność identyfikacji klientów oraz ustalenia pochodzenia środków finansowych,
- konieczne jest prowadzenie dokumentacji wszystkich transakcji,
- należy wyznaczyć Specjalistę ds. przeciwdziałania nadużyciom finansowym (Money Laundering Reporting Officer, MLRO),
- wszelkie podejrzane transakcje powinny być zgłaszane odpowiednim organom,
- należy prowadzić odpowiednie szkolenia wewnętrzne,
- należy prowadzić oceny ryzyka, stały monitoring oraz kontrolę.

Co więcej, podmioty przekazujące pieniądze podlegają także rejestracji w Financial Service Authority (FSA – Urzędzie Regulacji Rynków Finansowych – przyp. tłum.) na mocy ustawy Payment Services Regulations z 2009 roku (dotyczącej regulacji rynków usług finansowych – przyp. tłum.)

Po rejestracji podmiot otrzyma status:

- Approved Payment Institution (Zarejestrowana Instytucja Płatnicza – przyp. tłum.) bądź
- Small Payment Institution (Mała Instytucja Płatnicza – przyp. tłum.) (dotyczy podmiotów o obrotach poniżej 3 milionów funtów miesięcznie).

Wspomniana ustawa wymaga od podmiotów składania okresowych raportów do FSA w celu nadzoru.

Celem tego prawa jest przede wszystkim ochrona depozytów pieniężnych klientów, nie zaś walka z praniem brudnych pieniędzy.

Wykorzystywanie przedsiębiorstw świadczących usługi w zakresie zarządzania pieniędzmi przez przestępców

W Wielkiej Brytanii, MSB stanowią osoby prawne, jednak wymagają także oficjalnej rejestracji. Przedsiębiorstwa te mogą pełnić bardzo ważną rolę dla lokalnych społeczności, na przykład świadcząc usługi przekazywania pieniędzy lub wartości do innych miejsc na świecie, gdzie tradycyjny sektor bankowy nie jest w takim stopniu rozwinięty lub nie jest skuteczny.

Jednak nie można nie zauważyć, że podmioty te są także wykorzystywane w dużej mierze przez przestępców do procederu prania brudnych pieniędzy. Dzieje się tak w wyniku wielu czynników, w tym braku odpowiedniej dokumentacji (co rozwiązało uchwalenie ustawy Money Laundering Regulations), braku konieczności zgłaszania podejrzanych transakcji organom państwowym (ponownie, problem rozwiązała wspomniana ustawa), minimalne ryzyko utraty wpłacanych pieniędzy (po przyjęciu środki zostaną wypłacone w miejscu docelowym), a także możliwości wypłacenia środków w niemal dowolnym miejscu na świecie w krótkim czasie.

Znaki

W większości przypadków odbiorcy są zmuszeni do zidentyfikowania się i spotkania z przestępcą. Zdarzają się sytuacje, w których spotkanie nie jest konieczne (np. pozostawienie pieniędzy w określonym miejscu) w celu odebrania pieniędzy przeznaczonych do wyprania. Często jednak obie strony nie miały ze sobą do czynienia i nie znają się, co może powodować pewne trudności.

W celu zapobiegania problemom osoby należące do półświatka wykorzystują „znaki", które są używane w celu ujawnienia tożsamości odbiorcy innym przestępcom, mogą także służyć jako forma potwierdzenia odbioru gotówki przez odbiorcę – znak w formie banknotu jest w takiej sytuacji przekazywany przestępcy lub jego przedstawicielowi w czasie transakcji. Zwykle znakiem jest określony numer seryjny danego banknotu – najczęściej wykorzystuje się w tym celu banknot o nominale 5 funtów, jednak wykorzystywane są także inne nominały oraz waluty. Banknoty wykorzystywane w roli znaków stanowią własność odbiorcy, w związku z czym wielu z nich woli przekazać przestępcy banknot pięciofuntowy zamiast większych nominałów.

W sytuacji, w której wykorzystywane są znaki, kontroler może czasami zażądać przekazania numerów znaków przez odbiorcę. Odbiorca przekazuje następnie numery seryjne (całe lub częściowe – zazwyczaj wykorzystywane są pierwsze dwie litery i cztery ostatnie cyfry) banknotów znajdujących się w jego posiadaniu (pochodzących często z zebranej przez niego gotówki). Po ustaleniu z kontrolerem czasu i miejsca odbioru gotówki, kontroler przekazuje znak (numer seryjny banknotu) swojemu klientowi. Kiedy przestępca lub jego przedstawiciel spotyka się z odbiorcą, ten ostatni przekazuje mu banknot zawierający znak (przekazany przez kontrolera numer seryjny).

Następnie przestępca sprawdzi numer seryjny i porówna go z informacją podaną wcześniej przez kontrolera. Po potwierdzeniu tożsamości, odbiorca otrzymuje od przestępcy pieniądze. Przestępca może zdecydować się na zachowanie banknotu-znaku jako dowodu przekazania pieniędzy.

Banknoty pochodzące ze Szkocji i Irlandii Północnej

W niektórych śledztwach dotyczących prania brudnych pieniędzy wychodzą na światło dzienne duże ilości banknotów pochodzących ze Szkocji, a także pewne ilości środków płatniczych z Irlandii Północnej. Dzieje się tak pomimo tego, że sprawy dotyczą przede wszystkim Anglii. Nie obserwuje się dużej różnicy pomiędzy poziomem przestępczości w Anglii i w Szkocji, jednak duże ilości szkockich środków płatniczych znajdywanych w wyniku śledztw stanowią banknoty o niskich nominałach – 10- i 20-funtowe.

W Szkocji działają trzy banki, które mają prawo do emisji banknotów. Są to Bank of Scotland PLC, Clydesdale Bank PLC oraz The Royal Bank of Scotland PLC. W Irlandii Północnej działają cztery banki mające prawo do emisji banknotów: Bank of Ireland (UK) PLC, AIB Group (UK) PLC (działający pod nazwą First Trust Bank w Irlandii Północnej), Northern Bank Limited (działający pod nazwą Danske Bank) oraz Ulster Bank Limited.

Banknoty emitowane przez wymienione powyżej banki stanowią legalną walutę (patrz niżej) i są przyjmowane w całym Zjednoczonym Królestwie. Posiadacze banknotów emitowanych w Szkocji i w Irlandii Północnej podlegają takiej samej ochronie prawnej jak posiadacze banknotów wydanych przez Bank of England. Banknoty emitowane przez szkockie i irlandzkie banki nie stanowią legalnego środka płatniczego (także na terenie Szkocji i Irlandii Północnej). Podobnie banknoty wydawane przez Bank of England nie są legalnym środkiem płatniczym w Szkocji i Irlandii Północnej. W praktyce jednak problem legalności środka płatniczego nie ma żadnego wpływu na codzienne transakcje oraz na fakt przyjmowania tych banknotów przez podmioty. Wiele spośród pozostałych form płatności, takich jak czeki oraz karty debetowe także nie stanowią legalnych środków płatniczych. To, jakie środki płatnicze są przyjmowane zależy tylko i wyłącznie od obu stron biorących udział w transakcji.

Banknoty pochodzące ze Szkocji i Irlandii Północnej mogą być przyjmowane w całej Wielkiej Brytanii, jednak w praktyce zależy to od wielu czynników, wśród których można wymienić znajomość rzeczonych banknotów przez handlarza, odległość geograficzną, wzorce handlowe oraz chęć zrealizowania transakcji.

Banknoty szkockie i irlandzkie są wydawane wyłącznie przez określone banki w poszczególnych krajach (w tym przez bankomaty rzeczonych banków). Podobnie w Anglii i Walii funty szterlingi emitowane są tylko i wyłącznie przez angielskie banki. Banknoty szkockie i irlandzkie otrzymywane przez angielskie banki są odsyłane do banków odpowiedzialnych za ich emisję – nie są ponownie wydawane klientom.

Co więcej, szkockie banknoty nie są także zwykle wydawane zagranicznym instytucjom wymagającym funta szterlinga (na przykład w celu wymiany w kantorze) – w większości przypadków są to banknoty wydawane przez Bank of England. Dodatkowo zagraniczne kantory niechętnie przyjmują szkocką walutę. W związku z tym pozbycie się szkockich funtów jest niezwykle trudne za granicą – zwłaszcza w większych ilościach.

Nawet w Anglii, pomimo faktu, że angielskie instytucje przyjmują szkocką walutę, posiadanie pieniędzy drukowanych w Szkocji poza typowymi miejscami ich występowania może być podejrzane, zwłaszcza w sytuacji, w których występowanie tych banknotów nie jest typowe dla danego klienta banku.

To sprawia duże problemy przestępcom, którzy dokonują transakcji z przedstawicielami przestępczego półświatka w Szkocji lub Irlandii Północnej i wchodzą tym samym w posiadanie tamtejszych walut. W rezultacie tego typu banknoty bardzo często krążą pomiędzy przestępcami w ramach wielu transakcji. Z czasem ilość posiadanych pieniędzy pochodzących ze Szkocji i Irlandii Północnej znajdujących się w rezerwach grup przestępczych rośnie, ponieważ nie mają możliwości pozbycia się ich bez nadmiernych trudności lub wzbudzania nadmiernych podejrzeń.

Organizacje przestępcze działające na terenie Anglii mają do czynienia z tymi samymi problemami związanymi ze szkocką i irlandzką walutą, co wiąże się z pobieraniem przez nie większych opłat za przetwarzanie tych pieniędzy.

Komunikacja

Skuteczna komunikacja to podstawa działania każdej organizacji przestępczej zajmującej się praniem brudnych pieniędzy. W celu przekazywania informacji przestępcy wykorzystują faksy, telefony oraz komputery, a także spotkania twarzą w twarz i różne metody przekazywania dokumentów.

W przedstawionych powyżej systemach prania brudnych pieniędzy, komunikacja jest niezwykle ważna, gdyż umożliwia nawiązywanie kontaktu przez uczestników procederu, którzy często nie znają się nawzajem. Jak zostało opisane w niniejszym dokumencie, kontrolerzy są kluczowymi osobami w tego rodzaju organizacjach i to właśnie oni stoją w centrum komunikacji. Konieczny jest bowiem kontakt pomiędzy przestępcą, który potrzebuje skorzystać z usługi prania brudnych pieniędzy oraz kontrolerem lub jego koordynatorem. Konieczne jest także ustalenie warunków transakcji. Kontroler lub koordynator musi zdobyć pełną wiedzę dotyczącą ilości gotówki, którą należy dostarczyć lub odebrać oraz miejsca spotkania, konieczne jest także ustalenie odpowiednich opłat za transakcję. Po ustaleniu szczegółów transakcji kontroler musi skontaktować się ze swoimi współpracownikami, a przestępca ze swoimi przedstawicielami.

Jeśli obie strony ustaliły, że zostanie użyty znak, kontroler musi uzyskać od odbiorcy numer znaku. Następnie uzyskany numer musi zostać przekazany przestępcy, który z kolei przekaże go przedstawicielowi dostarczającemu gotówkę. Następnie kontroler musi powiadomić odbiorcę na temat miejsca odbioru gotówki (choć szczegóły spotkania mogą zostać także ustalone bezpośrednio pomiędzy odbiorcą i przestępcą; jeśli transakcje mają miejsce regularnie, może to także być standardowe miejsce spotkań), a także czasu spotkania i sposobu kontaktu z grupą przestępczą. Kontroler potwierdza także numer znaku, który ma zostać użyty przez przestępcę. Po odbiorze i przeliczeniu gotówki, odbiorca kontaktuje się z kontrolerem w celu potwierdzenia odbioru kwoty. Następnie kontroler informuje odbiorcę o sposobie, w jaki należy pozbyć się gotówki.

Tego typu ustalenia są zazwyczaj dokonywane telefonicznie, najczęściej przez wiadomości tekstowe zawierające kody pocztowe lub inne informacje określające miejsce spotkania (wielu odbiorców korzysta z systemów nawigacji satelitarnej w celu ustalania lokalizacji), a także numery znaków, numery kontaktowe i kwoty.

Ian Pemberton
Garda National Drugs & Organised Crime Bureau, Ireland

Financial investigation methods by the Irish Police Force and the international cooperation to fight financial fraud

Abstract

I think it would be appropriate for me to speak about the protecting the financial interests of the EU from an Irish perspective. I will give the audience an insight into the challenges met by Irish law enforcement in terms of financial crime. Irish law enforcement is regularly encountering new and more sophisticated methods of financial crime. Additionally, I will give the audience an understanding of Irish law enforcement agencies training methods in combating financial crime. Are we sufficiently equipped or is our training outdated. I would also like to speak about tools used by law enforcement in combating financial crime with particular emphasis on legislation.

I will then proceed to giving some examples of current investigations which span not only nationally but internationally. These particular examples are ones which international cooperation has been sought and proven beneficial.

Finally, I will speak generally about international cooperation from an Irish perspective. Mutual Assistance Requests (MLAT), Extradition, Intelligence, Police to Police are all methods of international cooperation used by Irish Law enforcement and I will touch on each of them generally using examples of success and/or problems encountered

I am a Detective Garda attached to An Garda Siochana which is Ireland's National Police force. Just to give you a brief history of my career, I Joined An Garda Siochana in 2001 and I qualified from the Police training college in March of 2003 with a Diploma in Policing Studies (now equates to an ordinary degree).

I was assigned to a busy Dublin suburb where I learned the basics regarding investigative techniques and methods. In January 2008 I moved into the Criminal Assets Bureau, which I will talk about later. I spent almost six years with the Criminal Assets Bureau before moving to Cyprus as part of an Irish peace keeping contingent with UNFICYP.

Upon my return from Cyprus I went into the Organised Crime Unit which was amalgamated soon to be amalgamated with the National Drugs Unit to form 'Garda National Drugs & Organised Crime Bureau' in 2015.

In January of this year (2017) I was asked to assist with creating a financial unit within the Garda National Drugs & Organised Crime Bureau. I will speak a bit later about this unit. So in total I have 16 years experience as a Police officer with the last 10 years predominantly spent investigating financial crime.

Today I'm going to speak about financial fraud typologies affecting Ireland. I will then speak about the training methods and investigative methods used by Irish law enforcement and show how Irelands law enforcement have come together to tackle financial crime. I will give you a number of examples of current investigations and show how our methodologies have succeeded. Finally, I will conclude briefly on the topic of international cooperation.

Ireland is like any other country in terms of the typologies of financial fraud which is currently being committed against its citizens, government and Irish exchequer. The word 'Fraud' covers a multitude of offences; theft, corruption, money laundering, cybercrime, tax evasion, credit card frauds and social welfare frauds.

I'm now going to speak about each to these subjects and expand slightly regarding the sub categories of each subject.

The word theft has a broad meaning. Certainly within the Irish Criminal Justice System it can suggest something as simple as a shoplifting offence or something as complex as the misappropriation of millions of Euro from a bank account. Thefts from each end of the scale are common occurrences in Ireland and something which Irish law enforcement is tasked with investigating daily. The majority of these sub categories such as; Deception, handling stolen property, false accounting, suppression of documents and forgery are all very common typologies of Fraud which are affecting the Irish economy on a daily basis.

But 'Fraud' has evolved into something more complex over the past decade and the Irish law enforcement have been moving quickly to ensure we keep up with it.

Over the past number of years Ireland has seen a significant increase in Corruption within the state. Irish law enforcement has investigated Government officials for accepting inducements to manipulate procedures. We have investigated allegations of Politicians accepting cash incentives for assisting developers regarding planning applications. The Irish Revenue Commissioners have charged Politicians with tax evasion. We have seen corruption within both Public and Private Sectors in Ireland for a variety of reasons such as;

Public Sector

- police officers giving information (rare),
- prison officers selling phones and drugs,
- civil servant selling information.

Private Sector

- bid rigging – a commercial contract is offered to a specific company, even though for the sake of appearance several companies also present a bid,
- procurement fraud – tenders/purchasing of goods etc which are manipulated by both the person tendering and a 'compromised person' within the procurement section.

Money Laundering is becoming a regular occurrence in terms of detection and investigation within the Irish law enforcement circle. Irish Police, Revenue and Customs have strong legislative powers to deal with the majority of typologies of money laundering. We have great

success in relation to cash seizures and there has been a significant rise in seizures of cash which are being exported out of the jurisdiction.

Additionally, through our STR/SAR reporting we are investigating an increasing amount of incidents where cash is being moved through bank accounts in attempts to clean it. Although Ireland was marginally criticised by the FATF (Financial Action Task Force) report in 2015 regarding investigations of this nature, I am happy to report a significant increase in this type of investigation.

The 'typical methods' of laundering, which law enforcement investigation teams are encountering, is the use of 'Professional People' such as solicitors, accountants who assist in the process of laundering by offering advice and ultimately assisting in the process. The use of pre-paid credit cards is something which causes problems for investigators as sometimes these cards can go unnoticed.

Money transferring systems such as Western Union, PayPal, Money Gram etc are all keen to assist law enforcement but unfortunately their policies and procedures can, in some instances, not only disappoint themselves but disappoint us as investigators.

An Garda Siochana are more frequently coming across virtual currencies. We have circulated an information leaflet to all Police officers via our internal computer system regarding the use of Bitcoin and other virtual currencies. Police officers within the Criminal Assets Bureau are currently conducting in-service training to all law enforcement agencies engaged in financial investigations and creating awareness of virtual currencies.

Money launderers of all levels are purchasing assets in an attempt to disguise the proceeds of crime. A common phenomenon in Ireland is the purchase of several high valued watches which the criminal fraternity are using as currency. Additionally, in an attempt to hide the true owner of an asset, property is registered a different name.

Cybercrime is something which is growing more and more within Ireland. Every week are encountering new and more sophisticated methods of cybercrime. The ones which have affected Ireland the most are CEO Frauds ('Bogus Boss' fraud) and Invoice re-direct. In December 2016 a local authority in Ireland (Government Agency) was the victim of a CEO Fraud which cost them €4.3 million. This money was wired to an Irish account and then immediately transferred to an account in Hong Kong. The Garda National Economic Crime Bureau was contacted immediately. Luckily, through excellent international cooperation the money was subsequently frozen in Hong Kong and eventually returned to Ireland. In this case an investigator from the Economic Crime Bureau had a contact within the Fraud Bureau in Hong Kong was privileged to have a direct number for them. Good International relationships are the key to success which is evident in this case.

Ransomware, Malware and DDoS (Denial of Service) attacks are common forms of Cyber attacks. Irish businesses are regularly hit with Ransomware attacks which cost the Irish business industry millions.

'Card not present' frauds are a common occurrence and are generally as a result of a card skimming scam, phishing scam, malware or virus. Then your card details are either cloned or sold on the darknet and used to purchase items online where the card is not required to be physically present for a purchase.

Ireland's tax system is regularly being targeted by criminals. Ireland is regularly being targeted by VAT Carousels (Missing traders). These frauds consist of a network of companies who (on paper) move high value goods and incur VAT credits, when the goods are moved to another company. The Revenue Commissioner commonly collects the VAT from the company who ends up with the product but this company disappears leaving Revenue at the loss of the VAT (which it has paid to the previous company). The Irish exchequer loses millions of Euro to this scam annually.

In addition to this, the Irish Revenue Commissioners fall victim to a variety of frauds such as, Payroll Schemes (which I will talk about later), under declaration of tax, non declaration of tax (hiding money) and VAT frauds.

Ininstances such as these, more often than not, the Police and Revenue conduct a joint operation to combat the fraud at hand and secure prosecutions.

ATM card frauds are currently being tackled by Irish law enforcement quite successfully. We have seen a variety of methodologies being used by criminals. From ATM skimming, card trapping, Shoulder surfing (obtaining a person's PIN number by looking over their shoulder), transaction reversal and Jackpotting (Infecting the ATM with Malware). The majority of the cards and their information are sold on the darknet. I'm sure anyone who has been on the darknet has seen these cards for sale.

Ireland's welfare system is one which is under constant attack. Ireland offers welfare to citizens for a number of reasons such as; Unemployment assistance, Jobseekers allowance, disability allowance, careers allowance and pension to name a few. The extent of the Frauds committed range from making false declarations, claiming welfare while in full time employment (cash in hand), fraudulently claiming disability, claiming welfare while resident outside the state, claiming welfare for a relative or claiming for a deceased relative.

One recent case in Ireland was the case of an 82 year old woman whom claimed over €200,000 over a period of 28 years. This lady claimed welfare under her own name and also used the name of her partner's deceased wife. This lady pleaded guilty at Ireland's Circuit Court but received a suspended sentence due to her age.

In 2016 the Department of Social Welfare received 20,000 reports of welfare fraud through their confidential line. To deal with the overwhelming amount of welfare fraud, the Irish Government set up a multiagency task force comprised of Police investigators and investigators from the Department of Social Welfare. This dedicated task force are committed exclusively to combating this form of fraud.

So what have the Irish Law enforcement done to tackle these typologies of fraud which are draining our society?

We EAT our staff... We Educate, create Awareness and Train.

Law enforcement are continuously up skilling themselves in terms of third level education. Not alone do we send law enforcement officers on specific courses (which I will talk about later) but privately, funding is available to law enforcement that participates in third level

courses. Law enforcement officers that undergo these courses are awarded Certification, Ordinary Degrees, B.A Degrees and Masters or equivalent depending on the course.

Awareness regarding new typologies of crimes is circulated to all law enforcement officers. Law enforcement officers use their internal data bases to create awareness regarding all aspects of policing, investigative tools, typologies and methodologies of crimes. An annual fraud conference is held in Ireland every year were law enforcement come together for discussions and seminars regarding fraud.

Training is provided to law enforcement on an ongoing and regular basis to keep up with evolving methods of financial crime. In service is provided to law enforcement ensuring best practice issues are kept and maintained surrounding investigative procedures. Training is provided on a number of topics on a regular basis.

Additionally, we have created specialised units within our law enforcement agencies that deal with specific types of fraud, terrorist financing, criminal assets etc.

Our Revenue and Customs officers have dedicated investigations units, our Social Welfare department have a multiagency task force set up to deal with welfare frauds.

Our National Police have the Garda National Economic Crime Bureau (Fraud/ML/Cybercrime), Criminal Assets Bureau (Non conviction forfeiture), Garda National Drugs & Organised Crime Bureau (Drug trafficking & M/L), Special Detective Unit (Terrorist Financing), Garda National Protective Services Bureau (Human trafficking).

In addition to this the Irish Police force has strategically placed additional support to the National Units nationwide. The Garda National Economic Crime Bureau has appointed highly qualified personnel nationwide (which I will speak about in a couple of minutes). The Criminal Assets Bureau has also appointed Divisional Asset Profilers to assist with the overloading work load.

As law enforcement, we ensure that each of us is kept up-to-date with new typologies of financial crime affecting Ireland. The Irish Police circulate information via a private Police Portal. Additionally, the Irish Police issue regular circular's regarding new legislation ensuring awareness to all members.

International cooperation is a vital tool used by law enforcement around the globe and without the assistance from our overseas colleagues we are nowhere near as effective. We are stronger together. This was evident in the story I told earlier regarding the CEO attack from a Government agency which would have cost the Irish exchequer 4.3 million Euro. That story alone is proof that together we are stronger and combined we can deal with any of these typologies of financial crime.

Legislation in Ireland is something which is under constant review by legislators and regular scrutiny by barristers. I believe that Ireland is strong in terms of the legislation enacted to deal with financial crime.

Ireland's Police recruits begin their training at the Garda Training College in Templemore, Co Tipperary. It is here that Police Officers learn the foundations regarding investigative techniques, legislation, interview techniques, court procedures. We train our Police officers to the highest standard and provide them with the tools required to combat all crimes including financial crimes.

Our recruits are taught subjects such as; Legal studies, Policing studies, Technical studies, Social studies, Communication studies, Irish language, Fitness and finally, they must complete a thesis as part of their programme. Garda recruits then graduate with a B.A in Policing.

This is how we train Police officers and provide them with the foundation required to investigate.

Moving onto our Specialised Units, I did speak about them briefly already but I want to now speak about them in a little bit more detail showing how each of them play a role in investigating financial crime.

The Garda National Economic Crime Bureau (GNECB) is Ireland leading fraud investigative bureau. The GNECB is divided into 5 sections each with its own remit for specific typologies of fraud.

1. Fraud Assessment Unit & Commercial Fraud Investigation Unit

   The Fraud Assessment Unit assesses each case that has been referred into the GNECB with a view to establishing if the case warrants investigation by GNECB. The Commercial Fraud Unit conducts investigations around white collar and corporate fraud.
2. Financial Intelligence Unit (FIU) & Money Laundering Investigation Unit (MLIU)

   The financial Intelligence Unit (FIU) is a national reception point for financial institutions and designated persons whom are obliged to submit suspicious transaction reports (STR/SAR) In turn the FIU is directly supported by the Money Laundering Investigation Unit. The number of STR/SAR's submitted to the FIU has doubled in numbers from 2012 to 2015 (12,390 – 21,682) and continue to grow. This is predominantly due to a change in legislation in 2010 and increased awareness.
3. Cheque, Payment Card, Counterfeit Currency and Advance Fee Fraud Investigation Unit
4. Computer Crime Investigation Unit
5. Corporate Enforcement

   The Office of the Director of Corporate Enforcement (ODCE) is another multiagency unit made up of Detectives from the Garda National Economic Crime Bureau, accountants, administrators and lawyers whose aim is to improve the compliance environment for corporate activity in the Irish economy by encouraging adherence to the requirements of the Companies Acts.

In conjunction with the GNECB national fraud investigators were introduced a number of years ago. These investigators were historically recruited by GNECB and trained to a standard that would relieve the GNECB of their ever growing work load. But more recently, and to deal with the increase in financial crime in Ireland the national fraud investigators now endure a strict interview process, their suitability is assessed and if successful they are put forward to undergo a one year University training course. The selected candidates are sent to UCD to partake in a one year Graduate Certificate in Forensic Computing & Cybercrime Investigation. This course known worldwide within law enforcement circles as UCD have compiled this course specifically and exclusively for law enforcement only.

Candidates for this course are taught the following subjects:

- Computer Forensics,
- Live data analysis,
- Online Fraud Investigations,
- Financial Fraud Investigations & Techniques,
- Legislation,
- Open Source Intelligence,
- Case Study.

Like any other university you must complete a number university examinations and several assignments including a case study which is related to a current ongoing investigation which the student has under taken.

The officers then graduate from UCD with a level 9 qualification (high qualification) equivalent to a Masters Degree.

These officers then return to their respective stations around the country and are highly qualified fraud investigators that offer operational support to the GNECB as required along with covering all and any fraud investigations within their respective Police Divisions.

The Criminal Assets Bureau (CAB) is a law enforcement agency in Ireland. The CAB was established with powers to focus on the illegally acquired assets of criminals involved in serious crime. The Bureau's statutory remit is to carry out investigations into the suspected proceeds of criminal conduct. CAB identifies assets of persons which derive, (or are suspected to derive), directly or indirectly from criminal conduct. It then takes appropriate action to deprive or deny those persons of the assets and the proceeds of their criminal conduct.

The CAB is a multiagency law enforcement agency made up officers from the national Police force, Revenue commissioners, Social Welfare Officers, analysts and solicitors.

CAB have legislation enacted specifically for CAB officers and they work on a non conviction based forfeiture with a civil burden of proof in the Irish High Courts. In addition to this they can investigate in three ways

1. Proceeds of Crime investigation
2. Tax investigation and possible assessment
3. Welfare investigation and possible assessment

CAB has gained the respect of law enforcement agencies around the globe and has worked closely with their counterparts in other jurisdictions. CAB has an excellent reputation and has relied on international assistance in numerous investigations.

CAB also used strategically placed Divisional Profilers to assist with cases nationwide. Again these Divisional Profilers are trained to a high standard although they do not undergo a University course.

But, the CAB officers themselves are constantly advancing in terms of learning. CAB officers are now trained by the University of Limerick in a course titled 'The Assets, Confiscation & Tracing Investigators Course and participants are awarded a B.A Degree upon successful competition of this course.

The Garda National Drugs & Organised Crime Bureau (GNDOCB) was established in 2015 when the Garda National Drugs Unit and the Garda Organised Crime Unit merged. The merge of these two national units inevitable as drugs and organised crime go hand in hand. Upon the formation of this new and elite Garda unit a number of sub units were formed within the GNDOCB to include a phone analysis unit, CCTV analysis unit and a Financial Asset Profiling and investigations unit.

I am delighted to say that due to my expertise and experience, not to mention qualifications, I was asked to assist with setting up this unit. The FAPIU was formed in January of 2017 and is currently the talk of the financial investigations sector within law enforcement due to its success. I will give an example of one of our ongoing cases in a moment.

What investigative tools do we use as law enforcement agencies?

One National Police Force – Ireland only has one Police force which makes investigating crimes easier in terms of crimes that span nationwide.

At the beginning of most major financial investigations, we as financial investigators always meet with our Financial Investigation Unit (FIU) (STR/SAR). The purpose of this meeting is to glean vital evidence in terms of potential financial accounts that may be held by the target and being able to establish money movements if STR/SAR exist.

Ireland's Police force gathers and compiles incredible data which is contained within the Garda Computer Intelligence system. As an investigator we should always look at the obvious prior to advancing our investigations.

As there is only one Police force, it makes the accessibility to specialised units only a phone call away. Notwithstanding the fact that intelligence lies within our own data bases but the specialised units may always have that little bit more. The majority of specialised units are contactable 24 hours a day.

We train our investigators in the use of 'Open Source Intelligence'. You would be surprised to see how many people have public accounts such as; Facebook, Instagram, Twitter etc.

If you can't find your target through open source... You'll find their wife/partner

Forensic Accountant's are a necessity in terms of conducting forensic analysis of a person's financial status (past and present). More often than not the use of a forensic accountant is something which is over looked simply due to a lack of understanding and experience. Unless you are a forensic accountant, I would not attempt to explain to a barrister, Judge or Jury that you conducted the analysis yourself.

State Agencies – Irish Police officers seem to forget that we have other strands of information at our disposal which is easily accessible. The information contained within our Revenue, Customs and Welfare offices are overwhelming. They are vital in the combat against a successful financial investigation in terms of being able to prove officially a person's income or lack of it.

Land Registry is a tool used by law enforcement across Ireland to establish the ownership of property within the state. Not alone does it show official records of whom the registered

owner is but it also shows past owners. On a separate note and relating to open source, Ireland introduced a 'Property Price Register' which is available online and allows you to see how much a property was sold for.

Company Registration Office (CRO) is Ireland's official registration office for all companies. Law enforcement use this service to compile company profiles regarding suspicious companies. The detail on submission forms to the CRO is invaluable. (Name, Address, Phone, email, tax agent, company address etc)

Ireland's law enforcement, particularly the Police force, maintain and excellent relationship with all financial institutions within the jurisdiction. This assists in being able to pick up a phone to someone from a financial institution in emergency circumstances.

Legislation plays a key part in financial investigations in Ireland. It is important to know it and be confident to use it. This helps you stay one step ahead. Be clever with your use of legislation **never** go outside the legislation and always ensure you're covered legally in every action you take. This is the key to a successful investigation.

We teach our financial investigators successful investigative technique; plan your investigation step by step. Ensure you know what you're investigating and advance accordingly.

Irish law enforcement is trained in effective interviewing strategies. This includes the interviewing of both suspects and witnesses. Training is done on a graduated system starting from level 1 and maturing to level 4. Level 1 and 2 is given to all Police officers. Level 3 is for investigators and consists of three weeks of intensive training involving both class room learning and role plays. Level 4 training is for supervisor level only and this aspect is for the coordination and planning of serious investigations.

Exhibits and exhibits officer are specifically trained to deal with exhibits and continuity of exhibits. In all complex financial frauds the number of exhibits obtained during the course of the investigation can amount to thousands. A dedicated exhibits officer is a vital tool used by law enforcement which in each and every case has proved effective.

Incident Room Coordinator (IRC) – this is a tool used by Irish investigators particularly involving large complex investigations. The IRC course is again a three week intense training course teaching investigators how to run and take charge of an investigation room. The basic function of an IRC is to open a 'jobs book' issue 'job sheets', take minutes, keep appraised of all aspects of the investigation, compile reports, never get involved directly with suspects or witnesses.

Senior Investigating Officer (SIO) – which is another 3 week course followed by case study submissions. This course is for Police officers of the rank of Inspector or over. The SIO has overall responsibility of the investigation and it is their job to oversee a team of investigators. This has proven to be an effective tool used by Police officers in management of complex investigations.

Knowing your limit – Something which we instil with our investigators is that you are not expected to know it all. There are plenty of experienced financial investigators within An Garda Siochana. Ask them.

The specialised units meet regularly (once a month) to discuss current trends of crime and offer assistance and support to each other in operations both past and present. This is important.

Ireland has an effective system for international cooperation. But don't take my word for it. The Financial Action Task Force published the Irish mutual evaluation report in September 2017, where they state that Ireland shows an upward trend in the number of requests for assistance received and made, which can be seen by the table.

Ireland provides a range of cooperation including; MLA, extradition and intelligence/ information. It is reported that Ireland has an effective system that provides an exchange of information of sufficient quality in a timely manner. It also states that Ireland demonstrated good cooperation internationally on Money Laundering and Terrorist Financing issues.

The DVD included in the book contains examples of three cases that took place in Ireland in which international cooperation played an important role. I will also present their results.

I have shown you the typologies of financial crimes affecting Irish and global economy. I have shown how Ireland educates law enforcement officers and provide the investigative tools necessary for combating financial crime. But specifically, the common theme throughout this presentation is international cooperation and its importance. As previously stated 'we are stronger together.

Ian Pemberton
Garda National Drugs & Organised Crime Bureau, Ireland

Metody prowadzenia dochodzeń finansowych przez policję Irlandii i międzynarodowa współpraca w walce z oszustwami finansowymi

Streszczenie

Myślę, że jestem odpowiednią osobą, która może opowiedzieć o ochronie interesów finansowych UE z perspektywy Irlandii. Przekażę słuchaczom/czytelnikom wiedzę na temat wyzwań, z jakimi borykają się irlandzkie organy ścigania w zakresie przestępstw finansowych. Irlandzkie organy ścigania regularnie stykają się z nowymi i bardziej wyrafinowanymi metodami przestępczości finansowej.

Ponadto przekażę publiczności wiedzę na temat szkoleń irlandzkich organów ścigania dotyczących wiedzy na temat metod walki z przestępczością finansową. Czy jesteśmy gotowi? Czy może nasze szkolenia nie przystają do naszych czasów? Chciałbym również odnieść się do narzędzi stosowanych przez organy ścigania w zwalczaniu przestępstw finansowych, ze szczególnym naciskiem na prawodawstwo.

Następnie przejdę do podania kilku przykładów trwających obecnie dochodzeń, które obejmują nie tylko sprawy krajowe, ale również międzynarodowe. Przedstawione sprawy stanowią przykłady sytuacji, w których Irlandia poprosiła o wsparcie międzynarodowe i je otrzymała z korzyścią dla siebie. Na koniec opowiem ogólnie o współpracy międzynarodowej z perspektywy irlandzkiej. Wnioski o wzajemną pomoc (MLAT), ekstradycja, wywiad czy współpraca sił policji stanowią metody współpracy międzynarodowej stosowane przez irlandzkie organy ścigania i zamierzam przedstawić ich ogólne omówienie, przedstawiając przykłady sukcesów lub napotkanych problemów.

Na początek pozwólcie państwo, że przedstawię krótki przebieg mojej kariery. Wstąpiłem do policji w 2001 roku, a w 2003 roku uzyskałem dyplom studiów policyjnych uczelni policyjnej, który obecnie stanowi odpowiednik standardowego stopnia naukowego. Obecnie pracuję jako detektyw An Garda Síochána – irlandzkich sił policyjnych.

Zostałem przydzielony do jednego z bardziej aktywnych przedmieść w Dublinie, gdzie nauczyłem się podstaw technik i metod dochodzeniowych. W styczniu 2008 roku zostałem przeniesiony do Biura do spraw Mienia Przestępczego, o którym powiem więcej w dalszej części mojej prezentacji. Pracowałem tam przez niemal sześć lat, zanim zostałem przeniesiony na Cypr jako część irlandzkiego kontyngentu pokojowego w ramach Sił Pokojowych ONZ na Cyprze (UNFICYP).

Po powrocie zacząłem pracować w Jednostce do spraw Przestępczości Zorganizowanej, która wkrótce została połączona z Krajową Jednostką ds. Przestępczości Narkotykowej i w 2015 roku stała się Biurem ds. Narkotyków i Przestępczości Zorganizowanej.

W styczniu 2017 roku zostałem poproszony o pomoc przy stworzeniu jednostki zajmującej się sprawami finansowymi działającej przy Biurze. Przedstawię ją bardziej szczegółowo w dalszej części prezentacji. Łącznie przepracowałem 16 lat jako oficer Policji, z czego w ciągu ostatnich 10 lat skupiałem się głównie na badaniu spraw związanych z przestępczością gospodarczą i finansową.

W tej prezentacji omówię typowe rodzaje nadużyć finansowych występujących w Irlandii. Następnie przedstawię także metody szkoleniowe i śledcze wykorzystywane przez irlandzkie organy ścigania, a także zaprezentuję w jaki sposób organy odpowiedzialne za egzekwowanie prawa połączyły siły w celu zwalczania przestępczości finansowej. Przedstawię także kilka przykładów prowadzonych śledztw i na tej podstawie pokażę, w jaki sposób nasze metody okazały się skuteczne. Prezentacja zakończy się tematem współpracy międzynarodowej.

Jeśli chodzi o typologię nadużyć finansowych popełnianych przeciwko obywatelom, rządowi oraz skarbowi państwa, Irlandia nie różni się niczym od innych krajów. Pojęcie „nadużycia finansowe" jest bardzo pojemne i mieści w sobie wiele rodzajów przestępstw: kradzież, korupcję, pranie brudnych pieniędzy, cyberprzestępczość, unikanie opodatkowania, oszustwa związane z kartami kredytowymi oraz wyłudzanie świadczeń socjalnych.

Omówię teraz pokrótce wszystkie te tematy i nieco rozwinę pojęcia określające wymienione przeze mnie kategorie przestępstw.

Pojęcie „kradzieży" ma bardzo szerokie znaczenie. W irlandzkim systemie prawa karnego może ono oznaczać zarówno proste i oczywiste występki, takie jak kradzieże sklepowe, a także złożone i trudne sprawy, jak na przykład sprzeniewierzenie milionów euro z konta bankowego. Przestępstwa kradzieży o różnej skali występują w Irlandii dość często, w praktyce krajowe organy ścigania zajmują się takimi sprawami codziennie. Większość podkategorii tego przestępstwa, takich jak między innymi oszustwo, paserstwo, fałszowanie księgowości, ukrywanie dokumentów i fałszerstwa są typowymi metodami nadużyć finansowych, które codziennie wpływają na gospodarkę kraju.

W ciągu ostatnich dziesięciu lat przestępstwa te stały się jednak dużo bardziej złożone, a organy ścigania w Irlandii stale robią wszystko, co w ich mocy, aby zagwarantować, że będą w stanie dotrzymać przestępcom kroku.

W ostatnich latach w Irlandii znacząco wzrosła liczba przypadków korupcji w organach rządowych. Irlandzkie organy ścigania prowadziły śledztwa skierowane przeciwko urzędnikom państwowym dotyczące przyjmowania łapówek w zamian za manipulacje przy procedurach. Prowadzono także śledztwa dotyczące podejrzeń skierowanych przeciwko politykom, którzy mieli przyjmować korzyści finansowe od deweloperów w zamian za pomoc przy uzyskaniu pozwoleń na budowę. Irlandzkie organy podatkowe oskarżyły polityków o unikanie opodatkowania. Obserwujemy także korupcję w sektorze prywatnym i publicznym w Irlandii, związaną między innymi z:

w sektorze publicznym

- udzielaniem informacji przez funkcjonariuszy Policji (rzadko),

- sprzedażą telefonów i narkotyków przez przedstawicieli służb więziennych,
- sprzedawaniem informacji przez funkcjonariuszy publicznych;

w sektorze prywatnym

- ustawianiem przetargów – sytuacje, w których kontrakty i zlecenia są oferowane konkretnym firmom, nawet jeśli inne firmy także przedstawiają swoje oferty w celu sprawienia wrażenia, że cały proces jest legalny,
- nadużyciami finansowymi związanymi z zamówieniami – zamówienia i przetargi są manipulowane przez osobę biorącą udział w przetargu oraz przekupioną osobę w dziale zamówień.

Pranie brudnych pieniędzy jest obecnie przestępstwem, które jest regularnie wykrywane przez irlandzkie organy ścigania i regularnie rozpoczynają się nowe śledztwa w tych sprawach. Zarówno siły policyjne, jak również służby celne i podatkowe posiadają silne uprawnienia pozwalające na skuteczne zwalczanie większości form prania brudnych pieniędzy. Udało nam się osiągnąć wiele sukcesów w zakresie zarekwirowanego majątku, ostatnio zaobserwowaliśmy także znaczne zwiększenie liczby przypadków konfiskaty gotówki eksportowanej poza granice kraju.

Dodatkowo dzięki zgłoszeniom STR/SAR prowadzimy coraz więcej dochodzeń dotyczących przypadków przesyłania pieniędzy przez wiele kont bankowych w celu ich wyprania. Pomimo tego, że Irlandia została w pewnym stopniu skrytykowana w raporcie FATF (Financial Action Task Force) z 2015 roku w związku z dochodzeniami w tego typu sprawach, mogę z dumą powiedzieć, że od tamtej pory ich liczba zdecydowanie wzrosła.

Typowe metody prania brudnych pieniędzy, z którymi regularnie stykają się krajowe służby obejmują między innymi korzystanie z usług profesjonalistów, takich jak prawnicy oraz księgowi, którzy pomagają przestępcom w procesie prania pieniędzy swoimi poradami, czasem nawet aktywnie uczestnicząc w procederze. Przestępcy używają także w tym celu przedpłaconych kart kredytowych, co stanowi pewne utrudnienie dla śledczych, gdyż często tego typu karty pozostają niezauważone.

Przedsiębiorstwa zajmujące się przekazami pieniężnymi, takie jak Western Union, PayPal, Money Gram i inne chętnie pomagają organom ścigania, jednak stosowane przez nie procedury i zasady w pewnych przypadkach zawodzą, ku niezadowoleniu zarówno wspomnianych serwisów, jak również śledczych.

Co więcej, An Garda Síochána coraz częściej styka się z wirtualnymi walutami. Wszyscy funkcjonariusze policji otrzymali niedawno informacje dotyczące waluty bitcoin oraz innych kryptowalut w wewnętrznym policyjnym systemie komputerowym. Dodatkowo, funkcjonariusze pracujący dla Biura do spraw Mienia Przestępczego organizują szkolenia dla wszystkich służb biorących udział w śledztwach dotyczących spraw finansowych, rozpowszechniają także informacje na temat kryptowalut.

Przestępcy zaangażowani w proceder prania brudnych pieniędzy używają ich do zakupu środków trwałych w celu ukrycia dochodów pochodzących z przestępstwa. Jednym z najczęściej obserwowanych rodzajów tego typu działań w Irlandii jest zakup zegarków o wysokiej wartości wykorzystywanych następnie w roli waluty przez członków przestępczego półświatka.

Co więcej, w wielu przypadkach tożsamość prawdziwego właściciela jest ukrywana poprzez rejestrację mienia pod innymi nazwiskami.

Także cyberprzestępczość jest zjawiskiem, które stale zyskuje na popularności w Irlandii. Każdego tygodnia stykamy się z coraz bardziej zaawansowanymi i wyrafinowanymi metodami przeprowadzania cyberataków. Wśród tego rodzaju oszustw i wyłudzeń, najpopularniejszymi i zdecydowanie najbardziej szkodliwymi są oszustwa „na szefa" oraz wyłudzenia polegające na przekierowaniu zapłat za faktury. W grudniu 2016 roku jedna z agencji rządowych padła ofiarą oszustwa „na szefa", straty wyniosły 4,3 miliona euro. Pieniądze trafiły na irlandzkie konto, skąd zostały natychmiast przelane na konto założone w Hongkongu. Poszkodowani natychmiast nawiązali kontakt z Biurem ds. Przestępczości Gospodarczej. Na szczęście dzięki doskonałej współpracy międzynarodowej pieniądze zostały zamrożone w Hongkongu i wkrótce potem zwrócone do Irlandii. W tym wypadku śledczy pracujący dla Biura ds. Przestępczości Gospodarczej miał szczęście posiadać bezpośredni numer do osoby pracującej w Agencji ds. Nadużyć Finansowych w Hongkongu. Jak doskonale pokazuje ten przypadek, budowanie dobrych kontaktów międzynarodowych jest kluczem do osiągania sukcesów na polu zwalczania tego rodzaju przestępczości.

Do typowych form cyberataków zaliczamy ataki przy użyciu oprogramowania typu ransomware i złośliwego oprogramowania, a także ataki typu DDoS (Distributed Denial of Service). Przedsiębiorstwa na terytorium Irlandii regularnie borykają się z atakami za pomocą oprogramowania typu ransomware, co powoduje wielomilionowe straty.

Popularne są także nadużycia typu „card-not-present", mające miejsce w wyniku wyłudzania informacji (phishingu), skimmingu, a także ataków przy użyciu złośliwego oprogramowania lub wirusów. W wyniku takich ataków przestępcy uzyskują dostęp do danych kart kredytowych, które są następnie klonowane lub sprzedawane na czarnym rynku (także w Internecie) i wykorzystywane w celu dokonywania zakupów w Internecie, korzystając z faktu, że sprzedawca nie wymaga fizycznej obecności karty przy dokonywaniu transakcji.

Także irlandzki system podatkowy stanowi często cel dla przestępców, jednym z głównych typów wyłudzeń podatkowych są karuzele VAT. Wyłudzenia te polegają na tworzeniu sieci spółek obracających (na papierze) dużymi ilościami towaru, otrzymując zwolnienia i zwroty podatku VAT z chwilą przekazania towaru kolejnej spółce. Zwykle przedstawiciele organów podatkowych pobierają podatek VAT od firmy, która otrzymuje towar, jednak w przypadku karuzeli podatkowej wyłudzająca firma znika, co powoduje, że skarb państwa traci należny podatek VAT, który został wypłacony poprzedniej spółce. W wyniku tego procederu irlandzki skarb państwa traci każdego roku miliony euro.

Co więcej, służby podatkowe w Irlandii padają także ofiarą wielu innych rodzajów wyłudzeń, takich jak między innymi wyłudzenia związane z wynagrodzeniami (o których opowiem w dalszej części prezentacji), składanie zaniżonych deklaracji podatkowych, ukrywanie nieopodatkowanych środków oraz wyłudzenia podatku VAT.

W takich przypadkach policja często łączy siły z organami podatkowymi w celu zwalczania tego rodzaju przestępczości i ścigania osób uczestniczących w tym procederze.

Od pewnego czasu irlandzkie organy ścigania radzą sobie naprawdę dobrze z problemem wyłudzeń i nadużyć związanych z bankomatami. Zaobserwowaliśmy wiele różnorodnych

technik i metod używanych przez przestępców, takich jak skimming kart płatniczych, blokowanie kart, podglądanie kodów PIN, wycofywanie transakcji oraz infekowanie bankomatów złośliwym oprogramowaniem. Większość danych zdobytych w ten sposób kart jest następnie sprzedawana w Internecie. Jestem całkowicie pewien, że każda osoba odwiedzająca tego rodzaju zakątki Internetu natrafiła przynajmniej raz w życiu na informacje o sprzedaży danych kart.

Także system pomocy społecznej działający w Irlandii jest regularnie celem prób wyłudzeń. Irlandia oferuje obywatelom pomoc społeczną w kilku sytuacjach, między innymi w formie zasiłków dla bezrobotnych, wsparcia dla osób poszukujących pracy, zasiłków dla osób niepełnosprawnych, emerytur i wielu innych świadczeń. Zakres wyłudzeń i nadużyć związanych ze świadczeniami pomocy społecznej obejmuje między innymi składanie fałszywych wniosków, próby uzyskania świadczeń pomimo posiadania zatrudnienia, próby wyłudzeń zasiłków dla niepełnosprawnych, próby uzyskania świadczeń w czasie przebywania poza granicami kraju, oraz uzyskiwanie świadczeń w imieniu innych osób, także zmarłych.

Jednym z ujawnionych niedawno przypadków tego typu nadużyć była 82-letnia kobieta, która w ciągu 28 lat skutecznie wyłudziła ponad 200 000 euro zasiłków, uzyskując je zarówno na siebie, jak również na nazwisko zmarłej żony swojego partnera. Kobieta ta przyznała się do winy w sprawie, która odbyła się w jednym z sądów okręgowych, jednak otrzymała karę w zawieszeniu w związku z podeszłym wiekiem.

W samym tylko 2016 roku Wydział Pomocy Społecznej otrzymał 20 000 zgłoszeń dotyczących wyłudzeń świadczeń i zasiłków na poufnej infolinii. W celu walki z olbrzymią liczbą prób wyłudzeń świadczeń i zasiłków rząd irlandzki powołał specjalną grupę zadaniową złożoną ze śledczych Policji i Wydziału Pomocy Społecznej, której celem jest zwalczanie wyłącznie tego rodzaju nadużyć i wyłudzeń.

W tym miejscu wypada zapytać: „co robią irlandzkie organy ścigania w celu zwalczania wszystkich przedstawionych rodzajów nadużyć i wyłudzeń?"

Odpowiem: edukujemy, uświadamiamy i szkolimy.

Każdego dnia funkcjonariusze organów ścigania szlifują swoje umiejętności i zdobywają wiedzę na studiach wyższych, nie tylko w ramach kursów, na które wysyłamy naszych funkcjonariuszy, lecz także prywatnie – dostępne są odpowiednie fundusze, które pozwalają na sfinansowanie udziału w tego rodzaju szkoleniach. Funkcjonariusze, którzy ukończą takie kursy otrzymują odpowiednie świadectwa, a także stopnie naukowe, w zależności od wybranego szkolenia.

Wiedza dotycząca nowych rodzajów i typów przestępstw jest na bieżąco przekazywana wszystkim funkcjonariuszom organów ścigania, którzy wykorzystują wewnętrzne bazy danych w celu gromadzenia i rozpowszechniania informacji na temat walki z przestępczością, narzędzi śledczych, rodzajów przestępczości oraz metod stosowanych przez przestępców. Każdego roku w Irlandii odbywa się także konferencja funkcjonariuszy na temat nadużyć i wyłudzeń, podczas której biorą udział w dyskusjach i seminariach poświęconych temu zagadnieniu.

Funkcjonariusze są także na bieżąco szkoleni w zakresie metod stosowanych przez kryminalistów. Dodatkowo prowadzone są także działania mające na celu dzielenie się najlepszymi

praktykami związanymi ze śledztwami i dochodzeniami. Regularnie organizowane są także dodatkowe szkolenia dotyczące różnorodnych tematów i zagadnień.

Co więcej, powołaliśmy także specjalne jednostki w ramach poszczególnych organizacji, których zadaniem jest zwalczanie określonych rodzajów nadużyć, a także walka z finansowaniem organizacji o charakterze terrorystycznym, konfiskowanie majątku pochodzącego z działalności przestępczej itd.

Służby podatkowe i celne dysponują także własnymi jednostkami dochodzeniowymi, zaś Wydział Pomocy Społecznej ma do dyspozycji specjalną grupę zadaniową do celów zwalczania wyłudzeń zasiłków i świadczeń.

Policja w Irlandii dysponuje między innymi Biurem ds. Przestępczości Gospodarczej (do walki z nadużyciami, praniem brudnych pieniędzy i cyberprzestępczością), Biuro ds. Mienia Przestępczego (przepadek mienia bez skazania), Biuro ds. Narkotyków i Przestępczości Zorganizowanej (zajmujące się przemytem narkotyków i praniem brudnych pieniędzy), Specjalną Jednostkę Detektywistyczną (do walki z finansowaniem organizacji terrorystycznych) oraz Biuro Ochrony (do walki z handlem ludźmi).

Dodatkowo funkcjonariusze mają do dyspozycji także wsparcie strategiczne krajowych jednostek w całym kraju. Biuro ds. Przestępczości Gospodarczej powołało w tym celu wysoko wykwalifikowane osoby w całym kraju – opowiem o tym za kilka minut. Biuro powołało także osoby zajmujące się profilowaniem majątku i środków w celu wsparcia funkcjonariuszy podczas pracy nad wielką liczbą spraw.

Jako funkcjonariusze organów ścigania dokładamy wszelkich starań, aby wszyscy byli na bieżąco z nowymi rodzajami przestępstw finansowych występujących w Irlandii. Z tego powodu irlandzka policja udostępnia informacje przy pomocy wewnętrznego portalu policyjnego. Dodatkowo wydawane są także regularne okólniki dotyczące nowych przepisów, dzięki którym wszyscy są w stanie na bieżąco aktualizować swoją wiedzę.

Współpraca międzynarodowa jest niezwykle ważnym narzędziem wykorzystywanym przez organy ścigania na całym świecie. W praktyce bez wsparcia naszych kolegów z innych krajów nie bylibyśmy w stanie być równie skuteczni jak obecnie. Razem jesteśmy silniejsi. Idealnie pokazał to przykład wspomnianego przeze mnie wyłudzenia, które mogło kosztować irlandzki skarb państwa 4,3 miliona euro. Już sama ta opowieść jest wystarczającym dowodem na to, że wspólnie możemy zdziałać dużo więcej, a współpracując z innymi jesteśmy w stanie skutecznie zwalczać niemal wszystkie rodzaje przestępczości finansowej.

Prawa uchwalane w Irlandii są stale monitorowane przez prawodawców, a także regularnie sprawdzane przez prawników. Uważam, że pod względem praw uchwalanych w celu walki z przestępczością finansową Irlandia radzi sobie naprawdę dobrze.

Nowi rekruci na funkcjonariuszy policyjnych rozpoczynają swoje szkolenie od uczelni policyjnej w Templemore w hrabstwie Tipperary. Tam przyszli funkcjonariusze policji zdobywają wiedzę na temat technik dochodzeniowych, obowiązującego prawa, technik przesłuchań oraz procedur sądowych. Szkolenie nowych funkcjonariuszy jest zgodne z najwyższymi standardami, dzięki czemu mają do dyspozycji wszelkie narzędzia potrzebne do walki z każdym rodzajem przestępczości, w tym także z przestępczością finansową.

Rekruci zdobywają wiedzę dotyczącą wielu przedmiotów, między innymi z zakresu prawa czy języka irlandzkiego, biorą także udział w zajęciach fizycznych, a cały program kończy się opracowaniem pracy naukowej. Ukończenie szkoły policyjnej wiąże się z otrzymaniem tytułu Bachelor of Arts (odpowiadającego licencjatowi – przyp. tłum.)

Tak przebiega szkolenie funkcjonariuszy policji i właśnie w ten sposób przekazujemy im wszystkie informacje i techniki potrzebne do prowadzenia skutecznych dochodzeń.

Teraz chciałbym powrócić na moment do tematu wyspecjalizowanych jednostek, o których wspomniałem nieco wcześniej. Postaram się bardziej szczegółowo nakreślić rolę poszczególnych jednostek w dochodzeniach związanych z przestępczością finansową.

Biuro do spraw Przestępczości Gospodarczej (GNECB) zajmuje czołową pozycję w zakresie dochodzeń dotyczących nadużyć finansowych. Jednostka ta dzieli się na pięć sekcji, spośród których każda zajmuje się określonymi rodzajami nadużyć.

1. Dział Oceny Nadużyć oraz Dział Dochodzeń ds. Oszustw Handlowych

   Dział Oceny Nadużyć ocenia, jak sama nazwa wskazuje, wszystkie sprawy trafiające do GNECB w celu ustalenia, czy w danym przypadku należy podjąć czynności dochodzeniowe. Dział Dochodzeń ds. Nadużyć Handlowych prowadzi dochodzenia związane z nadużyciami w przedsiębiorstwach i korporacjach.
2. Dział Wywiadu Finansowego (FIU) oraz Dział Dochodzeń ds. Prania Pieniędzy (MLIU)

   Dział Wywiadu Finansowego jest krajowym punktem odbioru, do którego instytucje finansowe i wyznaczone osoby fizyczne mają obowiązek przesyłać zgłoszenia podejrzanych transakcji (STR/SAR). FIU dysponuje bezpośrednim wsparciem Działu Dochodzeń ds. Prania Pieniędzy. Liczba zgłoszeń podejrzanych transakcji trafiających do FIU wzrosła w ostatnich latach dwukrotnie – z 12390 w 2012 roku do 21682 w 2015 roku – i stale rośnie. Dzieje się tak głównie w wyniku zmian w prawie, które zostały uchwalone w 2010 roku, a także zwiększonej wiedzy i świadomości na temat tego rodzaju przestępczości.
3. Dział Dochodzeń ds. nadużyć związanych z czekami, kartami płatniczymi, fałszywymi pieniędzmi i zaliczkami
4. Dział Dochodzeń ds. Cyberprzestępczości
5. Jednostka ds. Zwalczania Przestępczości Korporacyjnej

   Biuro Dyrektora Jednostki ds. Zwalczania Przestępczości Korporacyjnej (Office of the Director of Corporate Enforcement, ODCE) stanowi kolejną grupę zadaniową, w skład której wchodzą funkcjonariusze Biura ds. Przestępstw Gospodarczych, księgowi, administratorzy oraz prawnicy, której celem jest dbanie o przestrzeganie przepisów przez korporacje działające w Irlandii poprzez zachęcanie do przestrzegania przepisów zawartych w prawie spółek.

Kilka lat temu w związku z GNECB powołano także krajowych śledczych do spraw nadużyć. Śledczy ci byli rekrutowani przez GNECB i szkoleni w sposób pozwalający na odciążenie Biura w związku z coraz większą liczbą wpływających spraw. Jednak w ostatnim czasie w związku z koniecznością walki ze stale wzrastającą liczbą przestępstw finansowych krajowi śledczy przechodzą obecnie wymagające rozmowy kwalifikacyjne, po czym oceniane są ich

umiejętności. W przypadku, gdy ocena jest pozytywna, wysyła się ich na roczny kurs szkoleniowy odbywający się na uniwersytecie. Wybrani kandydaci są kierowani na uniwersytet w Dublinie (UCD) w celu wzięcia udziału w rocznym kursie podyplomowym dotyczącym informatyki śledczej i zwalczania cyberprzestępczości. Kurs ten został opracowany przez UCD na potrzeby organów ścigania i jest znany przez funkcjonariuszy na całym świecie.
W czasie kursu kandydaci zdobywają wiedzę dotyczącą następujących tematów:

- informatyka śledcza,
- analiza danych,
- techniki dochodzeniowe związane z oszustwami internetowymi,
- techniki dochodzeniowe związane z nadużyciami finansowymi,
- prawo,
- biały wywiad,
- studia przypadków.

Podobnie jak ma to miejsce w przypadku zwykłych uniwersytetów, uczestnicy kursu są zobowiązani do zdania odpowiednich egzaminów oraz zaliczenia wyznaczonych zadań. Jednym z nich jest opracowanie studium przypadku związanego z dochodzeniem podjętym przez studenta.

Funkcjonariusze kończący kurs UCD otrzymują kwalifikacje 9 stopnia, będące odpowiednikiem tytułu magistra.

Po ukończeniu kursu funkcjonariusze wracają na swoje komendy w całym kraju już jako w pełni wykwalifikowani śledczy do spraw nadużyć, wspierając GNECB w razie potrzeby, a także prowadząc wszystkie dochodzenia związane z nadużyciami i oszustwami we własnym oddziale.

Biuro ds. Mienia Przestępczego (CAB) jest kolejnym z organów ścigania działającym na terenie Irlandii. CAB skupia się przede wszystkim na środkach pozyskiwanych przez przestępców i pochodzących z przestępczości. Głównym celem Biura określonym w prawie jest prowadzenie dochodzeń, co do których istnieje podejrzenie, że pochodzą z przestępstwa. CAB identyfikuje majątki i środki osób uzyskane bezpośrednio lub pośrednio w wyniku przestępstw bądź co do których istnieją takie podejrzenia, podejmuje także wszelkie działania mające na celu uniemożliwienie wykorzystania lub pozbawienie rzeczonych osób środków pochodzących z przestępstw.

CAB jest jednostką zatrudniającą funkcjonariuszy policji, a także służb podatkowych, przedstawicieli Opieki Społecznej, analityków i prawników.

Co więcej, CAB korzysta ze specjalnych przepisów i uprawnień wprowadzonych na potrzeby tej jednostki, uczestnicząc w procesie konfiskaty majątków bez uprzedniego wyroku skazującego, z koniecznością udowodnienia zasadności przed sądem cywilnym. Poza tym Biuro może także prowadzić trzy rodzaje dochodzeń i śledztw:

1. śledztwa w sprawie majątków uzyskanych w wyniku przestępstwa,
2. śledztwa dotyczące podatków wraz z możliwymi ocenami,
3. śledztwa dotyczące świadczeń i pomocy społecznej wraz z możliwymi ocenami.

CAB cieszy się dużym poważaniem organów ścigania na całym świecie i ściśle współpracuje ze swoimi odpowiednikami w innych krajach. Co więcej, Biuro cieszy się doskonałą reputacją i wielokrotnie samo korzystało z pomocy organów innych krajów w swoich śledztwach.

CAB korzysta także z usług funkcjonariuszy zajmujących się profilowaniem, którzy pomagają w prowadzeniu spraw na terytorium całego kraju. Osoby te otrzymują stosowne przeszkolenie, jednak nie kończą kursu na UCB.

Oczywiście sami funkcjonariusze CAB stale poszerzają swoją wiedzę. Obecnie Uniwersytet w Limerick szkoli oficerów na specjalnym kursie dla zatytułowanym „Majątek, konfiskata i techniki dochodzeniowe", a osoby kończące kurs otrzymują tytuł naukowy Bachelor of Arts.

Biuro do spraw Narkotyków i Przestępczości Zorganizowanej (GNDOCB) powstało w 2015 roku w wyniku połączenia Krajowej Jednostki ds. Przestępczości Narkotykowej i Jednostki ds. Przestępczości Zorganizowanej. Połączenie tych dwóch jednostek było nieuniknione w związku z tym, że narkotyki i przestępczość zorganizowana są często tożsame. W wyniku ustanowienia nowej jednostki powołano do życia także pewną liczbę jednostek podległych GNDOCB, wśród których znajdują się między innymi jednostka zajmująca się analizą rozmów telefonicznych oraz zapisów z kamer przemysłowych, a także Jednostka Profilowania Środków Finansowych i Dochodzeń (FAPIU).

Jestem dumny z faktu, że dzięki mojej wiedzy, doświadczeniu i kwalifikacjach zostałem poproszony o pomoc w organizacji tej jednostki. FAPIU powstała w styczniu 2017 roku i pomimo wyjątkowo krótkiej kariery znalazła się na językach funkcjonariuszy zajmujących się przestępczością finansową z racji odniesionych sukcesów. Za chwilę przedstawię jedno z trwających obecnie śledztw.

Jakich narzędzi i technik śledczych używamy w poszczególnych biurach, jednostkach i agencjach?

Jednolite krajowe siły policyjne – Irlandia dysponuje jedną policją, co ułatwia prowadzenie dochodzeń i śledztw w sprawach przestępstw dotyczących całego kraju.

Na początku większości dochodzeń w sprawach związanych z finansami spotykamy się z Jednostką ds. Dochodzeń Finansowych (FIU) (STR/SAR). Celem tego spotkania jest uzyskanie kluczowych informacji na temat potencjalnych kont posiadanych przez przestępcę i możliwości prześledzenia przepływów finansowych, jeśli istnieją jakiekolwiek zgłoszenia STR/SAR.

Irlandzka policja gromadzi i zestawia olbrzymie ilości danych w systemach informatycznych Gardy. Jako śledczy w pierwszej kolejności zwracamy uwagę na najbardziej oczywiste rzeczy zanim na dobre zaangażujemy się w śledztwo.

Z racji tego, że Irlandia dysponuje jednolitą policją, wszystkie wyspecjalizowane jednostki są dostępne niemal natychmiast – wystarczy jeden telefon. Niezależnie od tego, że w bazach danych znajduje się ogromna ilość danych, zawsze istnieje szansa, że jednostki specjalne dysponują dodatkowymi informacjami. Większość spośród wspomnianych jednostek działa 24 godziny na dobę.

Funkcjonariusze śledczy są także szkoleni z zakresu technik białego wywiadu. Wśród najbardziej zaskakujących faktów jest to, jak wiele osób których przypadki badamy ma publicznie dostępne konta na Facebooku, Instagramie, Twitterze i innych serwisach społecznościowych.

Jeśli nie ma możliwości znalezienia celu... Najczęściej znajdujemy żonę, męża lub partnerów.

W celu przeprowadzenia analizy śledczej statusu finansowego podejrzanych osób wykorzystujemy umiejętności biegłych księgowych. W wielu przypadkach tego typu możliwości są całkowicie pomijane, dzieje się tak głównie z powodu braku zrozumienia i doświadczenia, aczkolwiek nie polecam próby wyjaśnienia sędziemu, prawnikom lub ławnikom, że cała sprawa opiera się na samodzielnie przeprowadzonej analizie.

Agencje państwowe – funkcjonariusze policji w Irlandii często zapominają, że mamy także do dyspozycji inne łatwo dostępne źródła informacji. Ilość danych zbieranych przez służby podatkowe i celne, a także opiekę społeczną jest przytłaczająca, często są one nieodzowne dla sukcesu śledztwa w sprawie przestępstw finansowych, ponieważ pozwalają udowodnić oficjalnie zgłoszone dochody podejrzanego lub ich brak.

Rejestry ziemi są kolejnym narzędziem wykorzystywanym przez organy ścigania w Irlandii w celu ustalania własności nieruchomości w kraju. Jest to wyjątkowo przydatne narzędzie, ponieważ zawiera nie tylko oficjalne zapisy dotyczące obecnego właściciela, ale także dane poprzednich właścicieli. Nawiązując do tematu białego wywiadu, niedawno w Irlandii został uruchomiony rejestr cen nieruchomości dostępny publicznie w Internecie, umożliwiający sprawdzenie cen sprzedaży nieruchomości.

Kolejnym źródłem danych wykorzystywanym przez organy ścigania jest Biuro Rejestracji Spółek (CRO), którego zadaniem jest rejestracja przedsiębiorstw i spółek w Irlandii. Policja korzysta z niego w celu budowania profili podejrzanych spółek i przedsiębiorstw. Informacje zawarte na formularzach zgłoszeniowych do CRO są często bezcenne, zawierają bowiem nazwiska, adresy, numery telefonów, adresy e-mail, adres rejestracji firmy, nazwisko agenta podatkowego itd.

Dodatkowo irlandzkie organy ścigania, przede wszystkim policja, pozostają w doskonałych stosunkach ze wszystkimi instytucjami finansowymi działającymi na terenie kraju. Dzięki temu bardzo często jesteśmy w stanie zwyczajnie zadzwonić do odpowiednich osób w instytucjach, kiedy wymagane jest działanie w nagłych sytuacjach.

Prawo odgrywa bardzo ważną rolę w kwestii śledztw finansowych prowadzonych na terenie Irlandii, z tego powodu niezwykle ważnym jest jego znajomość i pewność w stosowaniu jego przepisów. Dzięki temu możemy być o krok do przodu przed przestępcami. Kluczem jest, by umiejętnie stosować obowiązujące przepisy, ale **pod żadnym pozorem** ich nie łamać, a jednocześnie mieć pewność, że wszystkie podejmowane działania mają odpowiednie umocowanie prawne. Właśnie to jest kluczem do przeprowadzenia skutecznego śledztwa.

Wszyscy nasi śledczy uczą się jednej z najbardziej skutecznych technik dochodzeniowych – planowania śledztwa krok po kroku. W pierwszej kolejności należy upewnić się, z jaką sprawą mamy do czynienia, a następnie podejmować odpowiednie działania.

Dodatkowo, funkcjonariusze w Irlandii są także szkoleni w zakresie skutecznych technik przesłuchań, zarówno jeśli chodzi o świadków, jak i podejrzanych. Szkolenie to odbywa się w czterostopniowym systemie, poczynając od pierwszego stopnia. Wszyscy funkcjonariusze policji przechodzą pierwszy i drugi stopień szkolenia. Stopień trzeci jest zarezerwowany dla funkcjonariuszy śledczych i składają się na niego trzy tygodnie intensywnego szkolenia obejmującego zarówno zagadnienia teoretyczne, jak i praktyczne odgrywanie scenek. Stopień czwarty jest przeznaczony tylko i wyłącznie dla przełożonych i dotyczy zaawansowanej koordynacji i planowania działań śledczych.

Oficerowie dowodowi przechodzą dodatkowe szkolenia związane z materiałami dowodowymi i ciągłością dowodów. W przypadkach związanych z poważnymi naruszeniami, liczba dowodów zebranych w czasie śledztwa może przekroczyć kilka tysięcy, z tego powodu oficerowie dowodowi są niezwykle cennym zasobem organów ścigania – do tej pory często okazywali się nieodzowni.

Kolejnym narzędziem wykorzystywanym przez irlandzkich śledczych, w szczególności w przypadku złożonych śledztw jest Koordynator Śledczy (IRC). Aby wykonywać tę pracę, funkcjonariusze muszą ukończyć intensywny kurs trwający trzy tygodnie, podczas którego zapoznają się z tajnikami prowadzenia śledztwa. Do podstawowych obowiązków Koordynatora Śledczego należy otwarcie księgi zadań, koordynacja funkcjonariuszy, sporządzanie notatek, ocena postępów śledztwa, opracowywanie raportów i dbanie o to, by nigdy nie nawiązywać bezpośredniego kontaktu z podejrzanymi lub świadkami.

Starszy Oficer Śledczy (SIO) – praca na tym stanowisku wymaga ukończenia kolejnego trzytygodniowego kursu, a także opracowania studium przypadku, jednak udział w kursie wymaga uprzedniego uzyskania rangi Inspektora lub wyższej. Starszy oficer Śledczy jest odpowiedzialny za przebieg śledztwa i nadzór nad zespołem śledczym. Korzystanie z wiedzy i doświadczenia starszych oficerów śledczych często okazywało się nieodzowne w prowadzeniu trudnych i złożonych śledztw.

Wśród innych ważnych rzeczy należy wymienić świadomość swoich ograniczeń. Jedną z rzeczy, które staramy się wpoić wszystkim naszym funkcjonariuszom jest to, że nikt nie oczekuje od nich wiedzy absolutnej. An Garda Síochána zatrudnia wielu doświadczonych śledczych finansowych, dlatego nie powinni wahać się zadawać pytań w razie problemów lub wątpliwości.

Raz w miesiącu przedstawiciele specjalistycznych jednostek spotykają się w celu omówienia nowych zjawisk i trendów w przestępczym półświatku, a także oferowania wsparcia pozostałym jednostkom w trwających śledztwach. To jest niezwykle ważny aspekt pracy organów ścigania.

Irlandia posiada bardzo dobry i przede wszystkim skuteczny system współpracy międzynarodowej. Nie musicie wierzyć mi na słowo. We wrześniu 2017 roku FATF opublikowała raport z wzajemnej oceny, w którym znalazło się stwierdzenie, że Irlandia z coraz większą częstotliwością otrzymuje i przesyła prośby o wsparcie, co ilustruje także tabela.

Irlandzkie organy ścigania oferują innym krajom swoją pomoc i wsparcie w zakresie zwalczania procederu prania brudnych pieniędzy, a także ekstradycji przestępców oraz udostępniania danych. Według raportu irlandzki system wymiany informacji pozwala na szybkie uzyskiwanie informacji wysokiej jakości. Raport stwierdza też, że Irlandia wykazuje się doskonałą współpracą międzynarodową w zakresie prania brudnych pieniędzy i walki z finansowaniem organizacji terrorystycznych.

Na dołączonej do książki płycie znajdują się trzy przykłady spraw, które miały miejsce w Irlandii, w których ważną rolę odegrała międzynarodowa współpraca, zaprezentuję także ich wyniki.

W tej prezentacji przedstawiłem państwu rodzaje przestępczości finansowej, z którymi boryka się zarówno gospodarka Irlandii, jak również globalna. Opisałem także proces szkolenia funkcjonariuszy organów ścigania i narzędzia, dzięki którym są w stanie skutecznie zwalczać przestępczość. Jednak najważniejszym tematem poruszonym w całej prezentacji jest międzynarodowa współpraca i jej ogromne znaczenie. Jak powiedziałem wcześniej – razem jesteśmy silniejsi.

Giles Orton
University of Central Lancashire, UK

Training Methods for Officers Combating Crime in the UK

Abstract

'Training methods to combat crime' is a broad topic, and could be approached from many different angles. In this presentation, I want to focus on the approach that the UK police adopt not just in respect of training but 'developing' criminal investigators. I will provide an overview of how police are trained to conduct criminal investigations, based on the core investigative doctrine. I am going to describe the framework of training, namely the Professional Investigation Programme (PIP), and make reference to the specialist Fraud and Financial Investigative Training Programme. I will highlight the growing importance of "evidence based policing" in combating crime and the role of the College of Policing and higher education working in partnership in this endeavour. I will conclude that the UK police must continue to change the culture of policing so that the focus of evidence based policing demands a higher priority, however the signs are a positive step change for the future of the investigation of crime.

My name is Giles Orton and it is a great pleasure to attend your conference to speak on the subject of training methods for officers combating crime in the UK.

There is a growing body of academic work, which underpins many criminal investigation techniques. Whether you are a highly experienced fraud or financial investigator, or a front line officer, the quality of your investigation is paramount not only in the success of combating individual crimes, but also in the legitimacy of policing. Traditional classroom based training is still prevalent across police forces. There is a considerable amount of literature on the subject of investigation, for example, (Burkhart, 1980) who conducted studies in police training methods, which were unable to prove strong training school performance as being indicative of strong operational performance.

For many of us, who have been on many training courses over the years, will have your own views on how effective that training was in terms of your operational expertise. As can be seen from this slide, the relationship between knowledge and experience is highlighted in Stewart (1998), with the route to the top right hand side of the chart, the highly experienced investigator operating with high knowledge, is achieved through both experience on the job and a high level of knowledge. However it is my experience that the organisation is not culturally fixed in routinely allowing others to benefit from experience gained on the job, by taking part in evidence based policing reflective practise.

Quite late on in my career in the service, the importance of training and development was redefined. Most recently, the whole police training and development agenda has since been subsumed into the concept of 'professionalization of the UK police'.

When I joined the police, I was sent on a training course for fourteen weeks, I was trained in law and procedure. However, officers joining the police in the UK today have to pay for this training themselves, self-funded degree programme as a pre-join requisite is common place, and the direction of travel is that every officer will have undergraduate degree level training before they enter the police, and work is ongoing towards a police constable degree apprenticeship programme under the principles set out in the Police Education Qualifications Framework (PEQF). Additionally, entry routes into the police service have been changed to attract a wider pool of talent, so that prospective officers are now able to directly enter the police at senior ranks, or into specialised posts. These are important issues when we consider how this will impact on the 'criminal investigation'.

At the centre of the professionalization of the UK reform programme is the creation of the College of Policing. Like many professions such as nursing and the legal profession, it provides that the "college" is responsible for overseeing and developing excellence in training and development.

Working closely (and in tandem) with the "College", the organisation charged with the responsibility of encouraging improvement across policing in the UK, (across all 43 of our police forces, in England and Wales), is Her Majesty's Inspectorate of Constabulary (HMIC). In 2012, following an inspection, it was stated in their inspection report: 'Training was focused on procedures and the legal use of powers, rather than becoming an effective crime fighter. The emphasis is on removing risk, rather than proactive interventions. There is some evidence based knowledge taught but there is little evidence that is being applied on the ground.'

This reflects my own experience of police training, especially detective training in England. When I moved from uniform duties to the detective ranks, I attended a regional detective training facility and completed a ten-week classroom based course, which provided the opportunity to learn the law by rote and conduct relevant practical exercises. However, on reflection, little prepared me for the role of a detective. Although I would impart knowledge and support the development of those officers around me, little time was spent by me or colleagues reflecting, documenting and disseminating the vast amount of experiences that I encountered through a wide and varied career. The infrastructure, leadership and time was missing to carry out this important exercise on a routine basis. Therefore, it could be said that one of the key challenges to effective investigation is changing the organisational culture, to one, which is, more accepting of evidence based knowledge and its importance on positively influencing operational activity.

When things go wrong during police investigations, it is often front-page news. It feels as if it is always there, with regular reports dissecting and criticising the police. I think this is a reflection of the public interest in crime investigation, the requirement for 24/7 news, exacerbated by the instantaneous need for this news, with various social media platforms publishing "news" regardless of its accuracy or detail. There are far-reaching implications. Failed (or perceived failed) police investigations affect public confidence as well as having a damaging impact on victims and the communities who suffer.

In this slide, we can see two distinct cases, both of which involved highly complex investigations, played out under the constant watch of the news. The first is the picture of Assistant Commissioner of the Metropolitan Police, Mark Rowley who can be seen trying to deliver a press statement outside court, following a jury decision in a police shooting. The fallout from this shooting has been directly linked to a series of national riots in the UK in the summer of 2011. Whilst trying to deliver this message, members of the public were shouting 'murderer', which caused a usually calm and measured man, to lose his temper.

The second photograph is a newspaper report following the murder of Jo Yeates in Clifton, Bristol, and a case where a highly complex crime investigation led to the initial arrest of the wrong person. In fact, the male arrested was the landlord of the property where Jo lived. He was an unusual man, his details were leaked to the press, and he was wrongly portrayed as a demon, attracting national press coverage.

In instances such as this, the effectiveness of police investigations become a hot topic. We often see tightened controls and additional measures put in place curbing police powers and procedures. However, what is evident is that complex investigations and the changing nature of crime itself, the police officer role and responsibility in combating crime is changing.

The core investigative doctrine provides a definitive national guidance on the key principles of criminal investigation. In this document, it describes an investigation as 'an effective search for material to bring an offender to justice'. Therefore, officers are taught that an investigation is a search for the truth rather than just identifying an offender. However, this can be interpreted widely with many agencies other than the police involved and with an 'investigation' incorporating many disciplines. Therefore, combating crime successfully requires a multidisciplinary approach, which involves partners from all sectors. This, in turn, creates a more fragmented police environment where accountability and responsibility between agencies is more difficult to define.

Across any system of investigation you can experience trade offs, with truth being traded off against fairness and both against considerations of cost (Nobles and Schiff, 1997). In the UK, the norm is no investigation. In 2007, Carson identified that against a total of 12.9 m crimes committed in the UK, there are only 0.62 million prosecutions.

Different crimes have different levels of seriousness, chances of detection and priorities in decision-making processes.

In order to respond to such a significant and diverse range of reported crime, agencies use a triage process. Eck, 1983, states that crime can be seen in categories: self-solvers (those cases that are solved immediately), cases able to be solved with some investigatory effort, those that require considerable effort or cannot be solved at all. The category will inform decisions in the screening process. Through the triage process, different approaches of investigation are apportioned to different categories of crime. Crime is allocated by complexity, threat, risk, harm, vulnerability and impact factors.

Offences of fraud in the UK are reported directly to the government agency 'Action Fraud' regardless of the nature of the fraud or victim involved. The triage process for reported fraud takes place here. Action Fraud involves and encompasses the National Fraud Intelligence

Bureau, which provides a filter, and intelligence function. They provide intelligence packages to respective police forces. Currently, case files are distributed based on the location of victim.

In any investigation, it can be said that there are two critical factors: a legal framework and the investigative principles and mindset (Kirkby, 2011). The legal and ethical framework creates rules that ensure human rights are protected. Investigators are not permitted to abuse human rights of the suspect, or introduce flawed evidence, which results in an injustice. The English legal system, of course, is based on the adversarial system in which the prosecution must provide evidence sufficient to prove that the offender has committed the offence beyond all reasonable doubt. The prosecution, therefore, are asked to disclose all their evidence first as well as provide any other relevant evidence to the defence. Material that undermines the prosecution or assists the defence is included.

The defence is then able to challenge the evidence before considering whether to produce evidence themselves. This process often sees the victim or witness in a case open to a robust cross-examination. There is a significant amount of statutory provision which investigators must operate in and have a good working knowledge.

Whereas this creates the legal framework, it does not deliver an effective investigation. A considerable amount of expertise is required to do this, for example: ethical judgement is extremely important. Wright (2007) describes ethics as 'a set of beliefs, values or standards by which people regulate their conduct'. It is argued that doing the thing right is different from doing the right thing, and with any investigation, there are moral judgements to be made (Kirkby, 2011). The mindset of the investigator, therefore, embarking on an investigation is highly relevant.

The core investigative doctrine sets out issues affecting mindset. It provides for the investigator to avoid cognitive shortcuts, which are more likely to be used in the areas of uncertainty when information is ambiguous or unavailable. Furthermore, it identifies the possibility of the investigator being open to bias whether through a concept referred to as 'belief persistence', where once a belief is formed it is difficult to override it, or 'conformation bias' where decision makers actively seek out evidence to support their hypothesis and place less emphasis on evidence that refutes it. Therefore, the investigative principles and mindset are imperative where we consider the competence of investigators and the ability to combat crime.

It is taught that the criminal investigation has two methods: reactive and proactive investigation. The main differences between these two methods, of course, are that reactive investigations generally start with a discovery of a crime and the investigators seek to bring offenders to justice by discovering materials that identify suspects sufficiently to enable the court to determine their guilt. It requires interviewing victims, witnesses and suspects. Proactive investigations can start from an intelligence package identifying groups or individuals who are assessed as being involved in ongoing criminal activity. They are often generated as a result of the tasking and coordination (T&C) process, and allocated for further investigation. Intelligence packages may include crime pattern analysis, network analysis, operational intelligence assessment, problem profiles, market profiles, subject analysis, tactical assessment, criminal business analysis and tactical profiles.

Investigators usually use a range of covert surveillance techniques to link offenders to criminal enterprise complemented by financial investigations and forensic science techniques. Stelfox (2009) provides the investigator with the stages of an investigation as used in major investigations. Of course, every investigation is different and may require a different route. Activities within the framework denote investigative strategies such as the investigation evaluation stages where there are stages such as the initial investigation, suspect management, identifying investigative options and decision making stages. In a financial crime training setting, the same framework is modified and referred to as the Fraud Investigation Model (FIM) (City of London Police Economic Crime Academy 2017), which is reproduced in this slide. This model provides the investigator with structure to follow when considering how to respond to allegations of fraud, and reflects some of the challenges that the nature of fraud investigation present. It adds a number or additional elements to the original core investigative doctrine.

In a non-fraud crime, criminal activity occurs and the offence is generally reported. Following the report, there is a period of information gathering and investigation that results in enforcement action. Once the case has been investigated, prevention and disruption opportunities may be considered. This way may well be an effective response with a period of harm and loss being limited. However, with the fraud matter the dynamics are different. In this crime type, the fraud takes place and is reported while the data gathering takes place, due to the nature of the fraudster, further offences are generally committed. This increases the levels and period of harm. The fraudster may develop new types of fraud activity whilst the investigation process moves on. The use of cyber-enabled devices, many of which are portable, enables the fraudsters to continue unchecked, and victims, often the most vulnerable, are affected. Therefore, the model emphasises the importance of opportunities for early disruption and prevention and by doing so the harm and loss is significantly mitigated by reducing enablers and vulnerabilities that fraudsters use to perpetrate crimes.

In any crime investigation, the incoming information into the investigation is graded as to its relevancy, its reliability and its admissibility. The rules of evidence exclude certain types of information thought unreliable. The investigator can organise information to establish what information is present and what is missing using the 5WH formula: Who: can be the victim, witness or offender identified? Where: is it clear that the offence took place; What: has occurred by piecing together all available information; When: the need to establish the time frame highlighting significant events; What: reason was this offence committed, and is there sufficient information gathered to explain How the offence was committed (Kirkby, 2011)

As such, the investigation principles require for all investigations to include understanding of the investigation process, planning, decision making and how this can be influenced by the mindset. How investigative and evidential evaluation can assist the investigator to determine the value of the material gathered. The final aspect, overarching all of this is the importance of management expertise.

Professional Investigation Programme

Having explained some of the general principles of investigation training and wider impacts on the 'investigation', I now want to set out the training methods for officers investigating crime in the UK and the specialist fraud and financial investigator programme.

The Professional Investigation Programme (PIP) is a cradle to grave curriculum for all investigators (College of Policing, 2012). It is a development programme rather than a set of training courses. Access to each level of the professional investigation programme is based on skills, knowledge and experience. Whether an officer ultimately ends up investigating general crime, major or serious and organised crime or fraud or financial investigation, the career progress through this framework is compulsory.

Stage 1 is the foundation of the investigation, an essential accreditation for all employees investigating volume crime. This is a national accreditation, which requires an officer to complete an exam and a development programme. It includes a two week initial classroom based course and a student completes a work based portfolio, which is assessed against national occupational standards. The students are required to attend continual professional development and their investigation is based upon the foundations of core investigative doctrine principles that I have outlined. These foundations of investigation are essential for all staff involved in investigating priority and volume crime. Because the majority of officers undertaking the first stage are based within neighbourhood policing teams, this is a key aspect of training for officers.

The elements of neighbourhood policing (NHP) are said to be; targeted patrol, engagement (empowering community) and problem solving. The PIP programme is underpinned and complements academic research to the most effective strategies for NHP. Getting investigation right at the front line level is paramount, as we must not forget that all serious and organised crime takes place at a local level and intelligence flows from here.

The second stage on the ladder is the Professionalisation Investigation Programme 2, when investigators identify and achieve accreditation when investigating serious and complex crime. Factors, which may influence whether such crimes are serious and complex include: the use of violence, weapons and firearms, sexual assaults, serious financial gain or loss resulting from the crime, or crimes, which are conducted, by a number of persons in pursuit of a common purpose.

In order to be considered for the role, requires the officer having worked successfully at PIP one level and to be selected as a suitable candidate. Then they must take the national investigation exam. Successful candidates enter the initial crime investigation development programme, which can take twelve months to complete, and encompasses a three-week classroom based course. They are allocated a duty detective to oversee their development and must complete a comprehensive portfolio of evidence. Again, they must complete annual continual professional development accreditation thereafter.

The third stage and the final one I want to discuss today, involves investigation of any major or serious crime and is aimed at effective senior investigators to lead the investigation. As previously discussed, there is a great deal that any programme or training cannot teach and will only come from experience and exposure, and reflection following decision making.

The complex world of investigation for the senior investigator requires accreditation in the UK at PIP 3, whether a proactive policing route or reactive route is taken. Any specialist investigator involved in serious fraud, homicide, terrorism, or drug related matters, will progress through the PIP process before attending nationally accredited specialist portfolio training.

An important method of training within the PIP programme is the use of immersive learning. Immersive learning is the delivery technique designed to stimulate the reality of a critical incident management (College of Policing, 2012). Immersed in a realistic environment, students experience a decision making process and understand the complex issues involved. It delivers exercises for all ranks and levels within the service and partner agencies. Immersive learning uses the simulation system and methodology of Hydra to create life instances such as train derailments, plane crashes, riots or major crimes investigations. These exercises include public order command (at gold, silver and bronze levels), multi agency child protection and critical incident management for lower ranks. Immersive learning also uses a debriefing system.

The Specialist Fraud Investigation Programme is the National Investigator Programme for all officers involved in fraud across England and Wales. The course is predominantly a classroom-based course, held in a regional training school, delivered by Economic Crime Academy and City of London Police. It is a level 4 qualification for professional practice (and on the scale level 6 is undergraduate course). It is delivered by law, theory and practice based approach and topics such as bribery, corruption, fraud prevention and insolvency are introduced.

The financial investigation training and development is a career pathway, which starts out with the investigator attending a series of courses, which builds towards accreditation and the Financial Investigator (FI) 'Gateway' status. This accreditation provides the FI with the ability to speak directly with financial institutions to obtain information relevant to ongoing investigations. The career pathway for Financial Investigators is based upon a three, week long courses, including a foundation course, confiscation course and money laundering module. Additional courses are provided for field intelligence officers who have the specific financial investigation research capability.

The core investigative doctrine therefore is at the heart of taught criminal investigation throughout the PIP programme. As previously mentioned it provides investigators with processes and procedures to follow, against which to structure an investigation. At the start of any investigation, an investigator will identify possible hypothesis, the investigatory approach and develop strategy. I want to just touch on a few of these strategies to demonstrate the approach to training and its importance in combating crime as supported by academic research. I would argue that getting the basics right is fundamental to any investigation at whatever level.

Forensic Strategy

Investigators are taught first about a forensic strategy. Frazer (2008) identifies that forensic investigation is the integration of a range of scientific and technological evidence and intelligence in support of criminal investigations. Forensic investigation requires a structured cooperation between police investigative teams and a range of specialists to ensure effective outcomes. Only last week West Yorkshire Police (in the UK), a force in the North of England,

working together with Sheffield University academics, announced latest developments within techniques in fingerprint identification, whether the donor of the fingerprints left at a scene was (at the time they left the marks) did so whilst under the influence of drink or drugs. In one particular case they looked at, they identified the suspect's fingerprints from a scene studied 30 years earlier as having been under the influence of alcohol.

Trainee investigators are therefore taught the principles of forensic investigation, for example, Locard's transfer principle and particular importance it has in the process of developing or eliminating investigation hypothesis. In this slide, we are reminded of transfer principles as taught to police officers where the transference of samples can go either way. Either the person who leaves it, being a donor or a person that picks it up, being the receptor, and the secondary transfer, whilst not forgetting that the absence of evidence is not an evidence of absence. These theories are underpinned by knowledge of the type of material traces under consideration. Practical considerations across recovery of biological and physical samples from scene examinations are learnt. It is also worth remembering that skills of forensic scientists are just as much learned behaviour. In order to develop working practices between investigators and forensic science, all students at University of Lancashire are able to benefit from hands on learning through the recently completed Forensic Science Academy. One of the aims of this Academy is to promote a culture and the importance of evidence based approach to investigation.

Investigative Strategy

A key element in combating crime is the investigative interviewing process and I just wanted to touch on this, again, an area of investigation has been heavily influenced by academic support. Whether this is through reactive investigation interviewing victims or witnesses or in a proactive setting speaking to informants, investigative interview is a key strategy implemented by senior investigative officer. It is a consistent thread that runs through police training from levels PIP level1 to 3.

Police training focuses on interviewing, with a view to finding the truth and not to seek a convenient confession. This philosophy is an important shift influencing mindset. Interview training methods are based on the acronym PEACE which is described as: Preparation and Planning before the interview, Engagement and Explanation, inviting an initial Account, which maybe and hopefully does include, Challenge and Clarification, Closure including opportunity to add or Clarify, then finally a process of Evaluation. From my experience and observation, particularly at the first level of professional training, this structure provides a framework to guide, however significant opportunities are lost by officers sticking rigidly to this framework, missing those softer skills to enhance the flow of communication.

However, at the second stage of Investigator Training PIP 2, they will be more tuned into strategic approaches to interviewing suspects and have the opportunity to more advanced interview technique courses as part of the PIP programme. This training has been significantly informed by academic research an example being the learning about interviewing in strategic ways, addressing issues such as tactical advantages of increasing cognitive load during interview or the strategic introduction of evidence. This academic influence can

be seen in this slide, where we can see the guidance on dealing with deceptive practices in interviews from the perspectives of the deceiver and the detector. From early on an investigator can now benefit from important research around interviewing techniques. The habits of a deliverer, deceiver and actions an investigator should adopt within a framework of legal disclosure rules.

Passive data strategy

Another investigative strategy taught is that of the access and collection of passive data. The UK is reported to have the highest level of CCTV and other passive data sources in the world. However, there has been much criticism of the low volume of CCTV data used to support investigations and it is my personal belief that combating crime could be more effectively approached by Police in the UK through better training and resources invested in capturing evidence produced by this source. However, in major investigations, the investigator will set out a strategy for the collection. In this slide, Tilly (2007) identifies that in 18% of volume property crimes, a direct suspect is identified. Interestingly, the use of informants is only at 0.5%.

Intelligence strategy

Intelligence strategies are critical in combating crime. The National Intelligence Model provides a standardised approach to gathering, coordinating and disseminating intelligence, which can be integrated across all forces and law enforcement agencies. As can be seen from this slide, the model works on three levels:

Level 1 is intelligence at a local policing level; Level 2 is at a force and regional level and level 3 at a serious and organised crime level including national and transnational. Combating crime is dependent upon how information intelligence is assessed, both at a strategic and operational level to identify problem profiles and target the action.

The National Intelligence Model is taught to investigators, a model which enables the flow of intelligence and enables decisions to be made on priorities of crime and appropriate tactical responses. In this slide the complications of transnational nature of crime can be seen. The mobility of populations are compared whereas in 1950 twenty five million arrivals in the UK to now with over one billion arrivals in the UK. The increasing cross border mobility of people means many homicides, serious crime investigations including enquiries in one or more countries. This is particularly relevant to fraud and financial crime investigation settings. It is more likely that specialist teams within the framework of the National Crime Agency have a greater level of knowledge and provide special assistance to forces as there is no formal training in making enquiries abroad.

Any intelligence strategy works on the principle that every contact leaves a trace and as such, an investigator will set a strategy, which includes open source, passive data and covert sources and opportunities these present. No intelligence strategy is complete without consideration of the array of information intelligence and the financial footprint provides. This slide identifies opportunities to harvest intelligence to inform an investigation through a carefully considered and informed intelligence strategy.

In the UK, we have Financial Intelligence Officers working in Intelligence Units supporting any investigation work at all levels.

Investigators are taught that decision making on intelligence is not merely a simple linear process but requires collation and evaluation of evidence and information to ensure that investigative strategies have been completed. Officers are taught that a key tool in achieving this objective is the National Decision Model process. This cycle is a bedrock of investigative training in the UK and provides logical and structured approach to decision making in five stages. The cycle is utilised in arriving at decisions at the appropriate level of the investigation to be deployed regardless of its seriousness or complexity. It starts out with the gathering of information, identifying gaps in that information and then a plan of how these gaps will be filled, assessment of the risk and the development of a working strategy is the second stage followed by the consideration of the legal powers, policies and procedures. Options and contingencies to the approach will be taken and then the action is taken with a period of review. All of this is made on a cyclical basis at the centre of which there is a core statement of mission and values.

I have referenced the importance of the legal framework and the mindset of the investigator and implications for decision making.

The Professionalisation of Policing in the UK

This refers to a significant reform programme based upon the creation of the College of Policing. The ambition of the College of Policing is that everyone within policing is to have their professional academic endeavours recognised. The amount of courses I have attended over my service, which have not been formally recognised with a qualification leaves me reflecting on a wasted opportunity– this will not be a factor in the future. Set against the Police Educational Quality Framework, the future of British policing will require educational attainments for every officer from constable level, attaining a level 6 undergraduate degree qualification, through to superintendent ranks with a Masters level qualification and Chief Constable level with level 8 professional doctorate. This scope provides the organisation with an opportunity to further embed the evidence based policing agenda through important research capability and a work force that is capable of meeting future challenges by being provided with knowledge and skills beyond traditional policing methods.

The future, therefore, will enable a much closer integration of business, academia and professional policing to work together to combat crime, with a workforce that is professionally developed in tackling the challenges. It aims to attract a wider scope of applicants by opening up traditional routes into the organisation and to recognise a wider talent from all walks of life.

The role of higher education conducting research into policing problems across the UK is developing quickly, there are currently facilities up and down the country developing research on a wide variety of policing issues. This is a picture of one of the campuses within the University of Central Lancashire, where I work. We currently have PhD level research teams working on how police define, identify and respond to vulnerability. How to affectively assess the risk of domestic abuse, intimate partner violence and engagement with the police and whether the multiagency safeguarding hubs are an effective way to protect vulnerable

people. However, throughout the country, there is a work being developed on evidence based policing, and research projects.

Finally, I want to touch upon the offer at the University of Central Lancashire currently. We have Masters level programmes in Financial Investigation, Cyber Crime Investigation, Professional Practice and Early Intervention, Counterterrorism and Criminal Investigation. This brings together a range of students from business and academia. We currently have students from diverse range of business, including a solicitor from the International Criminal Court, from Barclays Bank and from other Financial Institutions currently on the Financial Investigator Masters Programme.

The University of Central Lancashire has a well established undergraduate and Masters programme, which has a truly international appeal. It caters for a wide range of learning preferences including distance learning. Although well subscribed and a very popular, this module thrives on the diversity of business, academia and law enforcement who partake.

Future aspirations include a forensic accounting courses, with direct relevance to fraud and financial investigation.

In conclusion, the link between academic research in supporting police operational activity is growing in its influence in the UK. Whilst at an operational level, it could be said that front line staff are not yet engaged in this reflective/evidence based approach, and police training still has some way to go to influence officers in this regard. The future senior leaders within the organisation may well be less experienced in operational experience, conducting criminal investigations, however by attracting a wider pool of talent and academic experience, it is for these leaders to continue to change the culture and influence all officers to engage in evidence based policing.

Giles Orton
University of Central Lancashire, Wielka Brytania

Metody szkoleniowe funkcjonariuszy zwalczających przestępczość w Wielkiej Brytanii

Streszczenie

„Metody szkoleniowe związane ze zwalczaniem przestępczości" to szeroki temat i można do niego podchodzić na wiele różnych sposobów. W tej prezentacji pragnę skupić się na podejściu brytyjskiej policji do problematyki zarówno szkolenia, jak i rozwoju funkcjonariuszy śledczych. Przedstawię przegląd tego, w jaki sposób funkcjonariusze policji są szkoleni do prowadzenia dochodzeń w oparciu o podstawową doktrynę dochodzeniową. Zamierzam także opisać ramy szkolenia – tak zwanego Professional Investigation Programme (PIP, Zawodowy Program Śledczy) – i odnieść się do specjalistycznego programu szkoleń dotyczącego śledztw i dochodzeń w zakresie oszustw i przestępczości finansowej (Fraud and Financial Investigative Training Programme). Podkreślę także rosnące znaczenie działań policyjnych opartych na wiedzy w walce z przestępczością oraz rolę College of Policing i szkolnictwa wyższego w tych działaniach. Moją prezentację podsumuję stwierdzeniem, że policja brytyjska musi w dalszym ciągu zmieniać kulturę działań policyjnych i zwiększać priorytet działań policyjnych opartych na wiedzy, jednak znaki stanowią ważną zmianę na rzecz przyszłości dochodzeń w sprawach przestępczości.

Nazywam się Giles Orton i cieszę się niezmiernie, że mogę uczestniczyć w tej konferencji i opowiedzieć państwu o metodach szkoleniowych funkcjonariuszy walczących z przestępczością w Wielkiej Brytanii.

Powstaje coraz większa liczba prac akademickich, które nadają kierunek wielu metodom prowadzenia dochodzeń w sprawach karnych.

Niezależnie od tego, czy mamy do czynienia z doświadczonym śledczym zajmującym się nadużyciami lub sprawami finansowymi czy też funkcjonariuszem działającym na pierwszej linii, jakość prowadzonego dochodzenia ma kluczowe znaczenie nie tylko dla powodzenia walki z poszczególnymi przestępstwami, ale również dla legitymizacji działań policyjnych. Tradycyjne szkolenia stacjonarne są nadal powszechne wśród sił policyjnych. Istnieje duża liczba prac dotyczących dochodzeń; przykładem może być Burkhart (1980), który prowadził badania dotyczące metod szkolenia funkcjonariuszy policji, które nie były w stanie dowieść, że dobre wyniki uzyskiwane w czasie szkolenia przekładają się na dobre wyniki operacyjne.

Wielu funkcjonariuszy, którzy przez wiele lat uczestniczyli w licznych szkoleniach, ma swoje własne poglądy na temat tego, jak skuteczne było ich szkolenie z punktu widzenia przygotowania operacyjnego. Jak widać na tym slajdzie, związek pomiędzy wiedzą i doświadczeniem

podkreśla Stewart (1998) – po prawej górnej stronie wykresu widzimy doświadczonego śledczego posiadającego szeroką wiedzę, który to wynik możemy osiągnąć zarówno poprzez doświadczenie w pracy, jak i wysoki poziom wiedzy. Z mojego doświadczenia wynika jednak, że w organizacji nie panuje jednak kultura wyciągania korzyści z doświadczenia zdobytego w pracy przez wyciąganie wniosków z działań policyjnych opartych na wiedzy.

Znaczenie szkolenia i rozwoju zostało zdefiniowane na nowo po upływie wielu lat mojej kariery w siłach policyjnych. Niedawno cały program szkoleń i rozwoju policji został włączony w koncepcję „profesjonalizacji policji brytyjskiej".

Kiedy wstąpiłem do policji, zostałem wysłany na trwające czternaście tygodni szkolenie, podczas którego zostałem przeszkolony w zakresie prawa i procedur. Pomimo to, funkcjonariusze dołączający dziś do sił policji w Wielkiej Brytanii muszą sami opłacać swoje szkolenie; powszechny jest samofinansowany program studiów jako warunek wstępny, a obecnym celem, do którego dążymy jest to, że każdy funkcjonariusz będzie musiał odbyć szkolenie odpowiadające stopniowi naukowemu licencjata zanim będzie w stanie dołączyć do policji. Prowadzone są także prace mające na celu opracowanie programu staży policyjnych zgodnie z zasadami określonymi w ramowym programie kształcenia policyjnego (Police Education Qualifications Framework, PEQF). Ponadto zmieniono również sposoby dostawania się do policji, aby przyciągnąć większą liczbę talentów. Dzięki temu potencjalni funkcjonariusze mogą teraz dołączyć do policji zaczynając bezpośrednio od wyższych stopni lub wchodząc na wyspecjalizowane stanowiska. Są to ważne kwestie, zwłaszcza jeśli weźmiemy pod uwagę ich wpływ na śledztwa.

W centrum profesjonalizacji ujętej w brytyjskim programie reform znajduje się założenie College of Policing. Podobnie jak w przypadku wielu zawodów, takich jak pielęgniarstwo lub zawody prawnicze, reforma zakłada, że nowe „kolegium" będzie odpowiedzialne za nadzorowanie i rozwój kompetencji w zakresie kształcenia i rozwoju.

Her Majesty's Inspectorate of Constabulary (HMIC) – brytyjski Inspektorat Policji – ściśle współpracuje z „kolegium policyjnym" jako organizacja, której celem jest promowanie poprawy systemu policji w całej Wielkiej Brytanii, obejmującego wszystkie 43 jednostki policyjne w Anglii i Walii. Po przeprowadzeniu inspekcji w 2012 roku powstało sprawozdanie, w którym znalazły się następujące informacje: „Szkolenia koncentrowały się przede wszystkim na procedurach i legalnym wykorzystaniu uprawnień, w mniejszym stopniu zaś na skutecznym zwalczaniu przestępczości. Nacisk kładzie się raczej na eliminację ryzyka niż na proaktywne interwencje. Część nauczanych informacji jest opartych na wiedzy, jednak istnieją zaledwie nieliczne przesłanki świadczące o tym, że są one stosowane podczas pracy w terenie".

Odzwierciedla to moje własne doświadczenia dotyczące szkoleń policyjnych, a zwłaszcza szkoleń dochodzeniowych w Anglii. Kiedy zmieniłem pracę i porzuciłem służbę mundurową na rzecz pracy dochodzeniowej, uczęszczałem do regionalnej placówki szkolenia dochodzeniowego, gdzie ukończyłem dziesięciotygodniowy kurs szkoleniowy, który dał mi możliwość nauczenia się prawa na pamięć i wzięcia udziału w odpowiednich ćwiczeń praktycznych. Odczuwam jednak, że kurs w niewielkim stopniu przygotował mnie jednak do pracy dochodzeniowej. Pomimo tego, że byłem w stanie przekazywać wiedzę i wspierałam rozwój otaczających mnie funkcjonariuszy, mało czasu spędziłam na myśleniu, dokumentowaniu

i rozpowszechnianiu ogromnej ilości doświadczeń zebranych w trakcie długiej i zróżnicowanej kariery zawodowej. Brakowało infrastruktury, przywództwa i czasu na rutynową realizację tego niezwykle ważnego zadania. Dlatego można powiedzieć, że jednym z kluczowych wyzwań dla skutecznego dochodzenia jest zmiana kultury organizacyjnej na taką, która umożliwia większą akceptację wiedzy opartej na dowodach i jej pozytywnego wpływu na działalność operacyjną.

Kiedy w czasie policyjnych dochodzeń cokolwiek idzie nie tak, skutkiem tego są zazwyczaj informacje na pierwszych stronach gazet. Czasem można odnieść wrażenie, że informacje tego typu nigdy tak naprawdę stamtąd nie schodzą i wszyscy ciągle krytykują policję, rozbierając każde jej działanie na czynniki pierwsze. Myślę, że stanowi to przejaw zainteresowania ludności kwestią dochodzeń kryminalnych, a także zapotrzebowania na aktualne wiadomości 24 godziny na dobę, spotęgowanych przez chęć natychmiastowego dostępu do najnowszych informacji i media społecznościowe wykorzystujące ten trend w celu publikacji tego rodzaju „wiadomości", niezależnie od ich dokładności i precyzji. Wiąże się to z daleko idącymi konsekwencjami.

Nieudane (lub postrzegane jako nieudane) dochodzenia policyjne mają negatywny wpływ na zaufanie publiczne, a także na ofiary i społeczności ponoszące konsekwencje przestępstw.

Na tym slajdzie widzimy dwa oddzielne przykłady – obie sprawy dotyczyły bardzo skomplikowanych dochodzeń, które były prowadzone pod czujnym okiem mediów. Pierwszym przykładem jest zdjęcie zastępcy komendanta policji metropolitalnej Marka Rowleya próbującego wygłosić oświadczenie prasowe przed budynkiem sądu po decyzji ławników dotyczącej strzelaniny z udziałem policji.

Skutki tej strzelaniny miały bezpośredni związek z serią zamieszek w Wielkiej Brytanii, które miały miejsce latem 2011 roku. Podczas gdy policjant próbował wygłosić oświadczenie, zebrani ludzie krzyczeli „mordercą", co powodowało, że ten zazwyczaj spokojny i wyważony człowiek stracił panowanie nad sobą.

Drugie zdjęcie to reportaż zamieszczony w gazecie po zabójstwie Jo Yeates w Clifton (Bristol) dotyczący sprawy, w której bardzo złożone dochodzenie w sprawie przestępstwa doprowadziło do aresztowania niewłaściwej osoby. W rzeczywistości aresztowany mężczyzna był właścicielem nieruchomości, w której mieszkała Jo. Był niezwykłym człowiekiem, jednak jego dane osobowe wyciekły do prasy i dodatkowo został niesłusznie przedstawiony jako wcielenie zła – temat odbił się szerokim echem w krajowej prasie.

W przypadkach takich jak te skuteczność dochodzeń policyjnych staje się gorącym tematem. Często obserwujemy zaostrzanie środków kontroli i wprowadzanie dodatkowych zasad i środków ograniczających uprawnienia i procedury policji. Oczywiste jest jednak to, że zarówno złożone dochodzenia, jak i zmieniający się charakter samej przestępczości powodują, że wraz z nimi także rola funkcjonariuszy policji i ich odpowiedzialność w walce z przestępczością muszą także ulec zmianie.

Podstawowa doktryna dochodzeniowa stanowi zbiór obowiązujących w kraju wytycznych dotyczących kluczowych zasad dochodzenia karnego.

Dokument ten określa dochodzenie jako „skuteczne poszukiwanie materiału pozwalającego na postawienie przestępcy przed wymiarem sprawiedliwości". Funkcjonariusze uczą się zatem, że śledztwo polega na dochodzeniu do prawdy, nie tylko na ustaleniu tożsamości przestępcy.

Zasadę tę można jednak interpretować na wiele sposobów w kontekście wielu agencji i organów innych niż policja oraz w kontekście „dochodzenia" obejmującego wiele dziedzin.

Dlatego też skuteczne zwalczanie przestępczości wymaga multidyscyplinarnego podejścia i uczestnictwa partnerów ze wszystkich sektorów. To z kolei tworzy bardziej rozdrobnione środowisko policyjne, w którym trudniej jest określić zakres i podział odpowiedzialności pomiędzy poszczególnymi agencjami.

We wszystkich systemach dochodzeniowych można zaobserwować kompromisy pomiędzy prawdą i sprawiedliwością, a także kwestiami związanymi z ich kosztem (Nobles i Schiff, 1997) W Wielkiej Brytanii normą jest niepodejmowanie dochodzenia. W 2007 r. Carson stwierdził, że pomimo tego, że liczba przestępstw popełnionych w Wielkiej Brytanii wyniosła 12,9 mln, wszczęto zaledwie 0,62 mln postępowań.

Różne przestępstwa charakteryzują się różnymi poziomami powagi, szansami wykrycia i priorytetem w procesach decyzyjnych.

Aby móc reagować na tak wielki i zróżnicowany zakres zgłaszanych przestępstw, agencje stosują wstępną selekcję – triage. Eck (1983) stwierdza, że przestępstwa można postrzegać, dzieląc je na następujące kategorie: sprawy, które rozwiązują się samoczynnie (sprawy, które są rozwiązywane natychmiast), sprawy, które mogą być rozwiązane w wyniku prostego dochodzenia, a także te, które wymagają znacznego wysiłku lub są nierozwiązywalne. Kategoria ta będzie stanowić podstawę decyzji podejmowanych w procesie selekcji. W ramach tego procesu do różnych kategorii przestępstw przyporządkowuje się różne koncepcje dochodzeń. Przestępstwa określane są pod kątem stopnia złożoności, zagrożenia, zagrożeń i ryzyka, szkody, wrażliwości i miary oddziaływania.

Nadużycia finansowe na terytorium Zjednoczonego Królestwa zgłaszane są bezpośrednio do agencji rządowej „Action Fraud", niezależnie od charakteru nadużycia lub jego ofiary. To właśnie tam dochodzi do wstępnej selekcji zgłoszonych nadużyć. Action Fraud obejmuje krajowe biuro ds. wywiadu i zapobiegania nadużyciom finansowym (National Fraud Intelligence Bureau), które odpowiada za filtrowanie spływających spraw oraz pełni funkcję wywiadowczą, dostarczając informacji wywiadowczych odpowiednim siłom policyjnym.

Obecnie akta spraw są dystrybuowane na podstawie miejsca pobytu ofiary.

Można powiedzieć, że w każdym dochodzeniu istnieją dwa kluczowe czynniki: ramy prawne oraz zasady i podejście dochodzeniowe (Kirkby, 2011). Ramy prawne i etyczne tworzą zasady zapewniające ochronę praw człowieka. Śledczy nie mogą w żaden sposób naruszać praw człowieka podejrzanego ani wnosić wadliwych dowodów, co prowadzi do niesprawiedliwości.

Brytyjski porządek prawny opiera się oczywiście na systemie kontradyktoryjnym, w którym prokuratura musi przedstawić dowody wystarczające do udowodnienia, że przestępca popełnił przestępstwo ponad wszelką uzasadnioną wątpliwość. Prokuratura ma zatem za zadanie ujawnienie w pierwszej kolejności wszystkich zebranych dowodów, a także dostarczenie obrońcom wszelkich innych istotnych dowodów. Włączony w to jest również materiał, który może podważyć linię oskarżenia lub pomóc obronie.

Obrona jest wtedy w stanie zakwestionować materiał dowodowy przed rozważeniem, czy wnieść do sprawy własne dowody. Proces ten umożliwia dokładne przesłuchanie ofiary lub

świadka przez obie strony. Istnieje znaczna liczba przepisów ustawowych, w ramach których muszą działać śledczy i o których muszą posiadać niezbędną wiedzę praktyczną.

Przepisy te tworzą ramy prawne, ale nie zwiększają w żadnym stopniu skuteczności dochodzenia.

W związku z tym wymagane są wiedza i umiejętności, wśród których bardzo ważną rolę odgrywa umiejętność oceny etycznej. Wright (2007) opisuje etykę jako „zbiór przekonań, wartości lub norm, według których ludzie regulują swoje postępowanie".

Argumentuje się także, że wykonywanie czynności we właściwy sposób różni się od robienia tego, co właściwe, a każde dochodzenie wymaga dokonania ocen i osądów natury etycznej (Kirkby, 2011). Postawa osoby prowadzącej dochodzenie jest zatem bardzo istotna.

Podstawowa doktryna dochodzeniowa określa kwestie wpływające na sposób myślenia i nastawienie. Zakłada ona, że śledczy powinien unikać skrótów poznawczych, które są bardziej prawdopodobne w przypadku niepewności, gdy informacje są niejednoznaczne lub niedostępne. Ponadto, identyfikuje ona możliwość, że śledczy może być podatny na bycie stronniczym, czy to poprzez zjawisko zwane „trwałością przekonań", które mówi, że po ukształtowaniu się przekonania trudno jest je zmienić, czy też poprzez tak zwany „efekt potwierdzenia", w wyniku którego decydenci aktywnie poszukują dowodów na poparcie swojej hipotezy i kładą mniejszy nacisk na dowody, które ją obalają. Dlatego też zasady śledcze i nastawienie są nadrzędne tam, gdzie rozważamy kompetencje śledczych i zdolność do zwalczania przestępczości.

Naucza się, że śledztwo karne opiera się na dwóch metodach: reaktywnej i proaktywnej. Najważniejsze różnice między tymi dwiema metodami polegają oczywiście na tym, że dochodzenia reaktywne zazwyczaj rozpoczynają się od wykrycia przestępstwa, a śledczy starają się postawić sprawców przed sądem odkrywając materiały, które pozwalają zidentyfikować podejrzanych w wystarczającym stopniu, by umożliwić sądowi ustalenie ich win. Metoda ta wymaga przesłuchiwania ofiar, świadków i podejrzanych. Proaktywne dochodzenia mogą rozpocząć się od informacji wywiadowczych określających grupy lub osoby, co do których istnieje podejrzenie, że są zaangażowane w działalność przestępczą. Są one często generowane w wyniku procesu przydzielania zadań i koordynacji (T&C) i przekierowywane do dalszego dochodzenia. Informacje wywiadowcze mogą obejmować analizę trendów i struktury przestępczości, analizę sieci, ocenę operacyjną wywiadu, profile problemów, profile rynkowe, analizę podmiotową, ocenę taktyczną, analizę działalności przestępczej i profile taktyczne.

Śledczy zazwyczaj stosują szereg niejawnych technik nadzoru, aby powiązać przestępców z organizacjami przestępczymi, w połączeniu z dochodzeniami finansowymi i technikami kryminalistycznymi. Stelfox (2009) przedstawia etapy dochodzenia wykorzystywane przez śledczych w najważniejszych dochodzeniach.

Oczywiście każde dochodzenie jest inne i może wymagać innego sposobu postępowania. Działania oparte na tych ramach oznaczają strategie dochodzeniowe, takie jak etapy oceny dochodzeń, podczas których występują etapy, takie jak dochodzenie wstępne, zarządzanie podejrzanymi, określanie możliwości dochodzeniowych i etapy podejmowania decyzji. Te same ramy zostały zmodyfikowane na potrzeby szkolenia w zakresie przestępczości

finansowej i nazywane są modelem dochodzenia w sprawie nadużyć finansowych (Fraud Investigation Model, FIM) (City of London Police Economic Crime Academy, 2017). Model ten został przedstawiony na tym slajdzie. Model FIM stanowi strukturę, na której powinien się wzorować śledczy rozważając sposoby reagowania na zarzuty nadużyć finansowych, i odzwierciedla niektóre z wyzwań, jakie niesie ze sobą charakter dochodzenia w sprawie nadużyć finansowych. Dodaje on pewną liczbę dodatkowych elementów do podstawowej doktryny dochodzeniowej.

W przypadku przestępczości niezwiązanej z nadużyciami finansowymi ma miejsce działalność przestępcza i przestępstwo jest zazwyczaj zgłaszane. W następstwie zgłoszenia rozpoczyna się okres gromadzenia informacji i prowadzone jest dochodzenie, którego wynikiem są działania związane z egzekwowaniem prawa.

Po zbadaniu sprawy możliwe jest rozważenie możliwości prewencji i zakłócenia działalności przestępczej. Dzięki temu możliwa jest skuteczna reakcja, dzięki której może zostać ograniczony okres szkód i strat. Jednak w przypadku nadużyć finansowych mamy do czynienia z inną dynamiką. W przypadku tego rodzaju przestępczości po zgłoszeniu i podczas gromadzenia informacji popełniane są na ogół kolejne przestępstwa ze względu na charakter przestępcy. Zwiększa to poziom i okres szkód. Co więcej, przestępcy mają dzięki temu możliwość rozwinięcia nowych działalności przestępczych w trakcie trwania dochodzenia. Korzystanie z urządzeń podłączonych do Internetu, w tym urządzeń przenośnych, umożliwia oszustom kontynuację działalności przestępczej, która prowadzi do poszkodowania ofiar, często wśród najbardziej narażonych osób. Dlatego też model ten podkreśla znaczenie możliwości zakłócenia działalności przestępczej na wczesnych etapach dochodzenia, a także prewencji, tym samym znacznie zmniejsza szkody i straty poprzez zmniejszanie możliwości i podatności na zagrożenia, które oszuści wykorzystują do popełniania przestępstw.

W każdym dochodzeniu kryminalnym informacje dotyczące śledztwa są oceniane pod względem ich istotności, wiarygodności i dopuszczalności. Zasady dowodowe wykluczają pewne rodzaje informacji, które są uważane za niewiarygodne. Przy pomocy formuły 5WH (której nazwa pochodzi od pytań w języku angielskim – Who, Where, What, When, What – przyp. tłum.) śledczy może zorganizować informacje w celu ustalenia, które informacje są dostępne i jakie informacje należy uzyskać: kto: czy można zidentyfikować ofiarę, świadka lub przestępcę? Gdzie: czy jest jasne, że przestępstwo miało miejsce; co: jakie zdarzenie miało miejsce na podstawie zebrania wszystkich dostępnych informacji; kiedy: potrzeba ustalenia ram czasowych i zaznaczenia wszystkich istotnych wydarzeń; co: dlaczego zostało popełnione to przestępstwo oraz czy zebrano wystarczającą ilość informacji wyjaśniających, w jaki sposób dane przestępstwo zostało popełnione (Kirkby, 2011).

W związku z tym zasady prowadzenia dochodzeń wymagają, aby we wszystkich śledztwach uwzględnić rozumienie procesu dochodzenia, planowania i podejmowania decyzji, a także możliwy wpływ nastawienia na cały proces. Dodatkowo należy też wziąć pod uwagę to, w jaki sposób ocena dochodzeniowa i dowodowa może pomóc śledczemu w określeniu wartości zgromadzonych materiałów. Ostatnim, nadrzędnym aspektem, jest znaczenie wiedzy i doświadczenia w zakresie zarządzania.

Zawodowy Program Śledczy

Po wyjaśnieniu niektórych ogólnych zasad szkolenia śledczego i szeroko rozumianego wpływu na proces dochodzenia, chciałbym teraz przedstawić metody szkolenia funkcjonariuszy śledczych prowadzących dochodzenia w sprawach przestępczości w Wielkiej Brytanii oraz specjalistyczny program szkoleniowy dla śledczych zajmujących się nadużyciami i przestępczością finansową.

Zawodowy Program Śledczy (PIP) jest kompleksowym programem nauczania dla wszystkich śledczych (College of Policing, 2012). PIP jest przede wszystkim programem rozwojowym, nie jest wyłącznie zestawem szkoleń. Dostęp do każdego poziomu programu opiera się na umiejętnościach, wiedzy i doświadczeniu. Niezależnie od tego, czy funkcjonariusz będzie zajmował się dochodzeniami dotyczącymi ogólnej przestępczości, poważnych przestępstw, przestępczości zorganizowanej lub nadużyć finansowych, przejście przez kolejne szczeble jest obowiązkowe.

Etap 1 dotyczy podstawowej wiedzy śledczej i stanowi zasadniczą akredytację dla wszystkich pracowników prowadzących śledztwa w sprawach przestępstw na dużą skalę. Jest to akredytacja krajowa, która wymaga od funkcjonariusza zdania egzaminu i ukończenia programu rozwojowego. Program ten obejmuje dwutygodniowy teoretyczny kurs wstępny i uzupełnienie przez studenta portfolio opartego na wykonywanej pracy, które jest oceniane według krajowych standardów zawodowych. Studenci są zobowiązani do ciągłego rozwoju zawodowego, a prowadzone przez nich śledztwa opierają się na podstawowej doktrynie dochodzeniowej, która została nakreślona wcześniej. Fundamentalna wiedza dotycząca dochodzenia ma zasadnicze znaczenie dla wszystkich pracowników zaangażowanych w prowadzenie dochodzeń w sprawach dotyczących przestępstw o znaczeniu priorytetowym i przestępczości na dużą skalę. Ponieważ większość funkcjonariuszy podejmujących pierwszy etap szkolenia pracuje w lokalnych zespołach policyjnych, jest to kluczowy aspekt szkolenia oficerów.

Mówi się, że elementami pracy lokalnych zespołów policyjnych są: ukierunkowane patrolowanie, zaangażowanie (wspieranie społeczności lokalnych) i rozwiązywanie problemów.

Program PIP jest oparty o badania akademickie i uzupełnia je, aby umożliwić tworzenie najbardziej optymalnych strategii pracy lokalnych zespołów. Nadrzędne znaczenie ma właściwe prowadzenie dochodzeń na pierwszej linii, ponieważ nie wolno nam zapominać, że cała poważna i zorganizowana przestępczość ma miejsce na szczeblu lokalnym i to właśnie stamtąd napływają informacje wywiadowcze.

Drugim szczeblem drabiny jest PIP 2, w ramach którego śledczy identyfikują i uzyskują akredytację w ramach prowadzenia dochodzeń w sprawach poważnej i złożonej przestępczości. Czynniki, które mogą mieć wpływ na to, czy dane przestępstwa są uznawane za poważne i złożone obejmują: użycie przemocy, broni i broni palnej, napaści seksualne, osiąganie dużych korzyści finansowych lub duże straty finansowe wynikające z przestępstwa lub wielu przestępstw popełnianych przez szereg osób w dążeniu do wspólnego celu.

Warunkiem możliwości ubiegania się o takie stanowisko jest skuteczna praca funkcjonariusza na pierwszym poziomie PIP i otrzymanie nominacji. Następnie kandydat musi przystąpić do krajowego egzaminu śledczego. Kandydaci, którzy pomyślnie zdają egzamin są kierowani na wstępny program rozwojowy dotyczący dochodzeń kryminalnych, którego

ukończenie może trwać do 12 miesięcy i obejmuje trzytygodniowy kurs stacjonarny. W celu nadzorowania ich rozwoju kandydaci współpracują z pracownikiem śledczym, a dodatkowo muszą także zebrać wyczerpujący zbiór dowodów. Od tamtej pory muszą także uzyskiwać akredytację ciągłego doskonalenia zawodowego każdego roku.

Trzeci i ostatni etap, który pragnę dziś omówić, obejmuje śledztwa w sprawie wszelkich poważnych przestępstw i ma na celu przydzielanie prowadzenia śledztw wyłącznie najbardziej doświadczonym śledczym. Jak już wcześniej wspomniano, jest wiele rzeczy, których nie jest w stanie nauczyć żaden program lub szkolenie i które będą oparte wyłącznie na doświadczeniu, a także z refleksji po podjęciu decyzji. Dostęp do złożony świata dochodzeń w Wielkiej Brytanii wymaga od doświadczonych śledczych akredytacji PIP 3, niezależnie od tego, czy wybierają działania proaktywne, czy reaktywne. Każdy wyspecjalizowany śledczy zajmujący się poważnymi nadużyciami finansowymi, zabójstwami, terroryzmem lub sprawami związanymi z narkotykami będzie kontynuował proces PIP przed przystąpieniem do akredytowanego na szczeblu krajowym szkolenia specjalistycznego w zakresie danych spraw.

Ważną metodą szkolenia w ramach programu PIP jest uczenie się poprzez doświadczanie. Nauka w oparciu o doświadczanie jest techniką nauczania zaprojektowaną w celu symulowania rzeczywistości zarządzania krytycznymi incydentami (College of Policing, 2012). Przebywający w realistycznym środowisku uczniowie doświadczają na własnej skórze procesu podejmowania decyzji i rozumieją związane z tym złożone procesy. Proces ten zapewnia ćwiczenia dla wszystkich szczebli w agencjach i jednostkach partnerskich. Uczenie się przez doświadczanie wykorzystuje system symulacji i metodologię opracowaną przez Fundację Hydra do tworzenia przykładów sytuacji życiowych, takich jak wykolejenia pociągów, katastrofy lotnicze, zamieszki czy śledztwa w sprawie poważnych przestępstw. Ćwiczenia te obejmują dowodzenie związane z utrzymaniem porządku publicznego (na poziomie złotym, srebrnym i brązowym), ochronę dzieci przez przedstawicieli wielu agencji oraz zarządzanie krytycznymi incydentami dla funkcjonariuszy niższych rangą. Uczenie się przez doświadczanie wykorzystuje również system odpraw i omówień.

Specjalistyczny program dochodzenia w sprawach nadużyć finansowych (Specialist Fraud Investigation Programme) jest krajowym programem dla wszystkich funkcjonariuszy zaangażowanych w prowadzenie spraw dotyczących nadużyć finansowych w Anglii i Walii. Kurs opiera się w dużej mierze na zajęciach stacjonarnych odbywających się w regionalnej jednostce szkoleniowej, prowadzonych przez Economic Crime Academy i City of London Police. Kurs ten stanowi czwarty poziom kwalifikacji do służby zawodowej (na skali poziom szósty odpowiada tytułowi licencjata). Jest on realizowany w oparciu o podejście oparte na prawie, teorii i praktyce; wprowadza zagadnienia takie jak łapownictwo, korupcja, zapobieganie nadużyciom finansowym i niewypłacalność.

Szkolenie i rozwój w dziedzinie dochodzeń finansowych to ścieżka kariery, która rozpoczyna się od uczestnictwa funkcjonariusza śledczego w szeregu kursów, których celem jest uzyskanie akredytacji i wstępnego statusu śledczego ds. finansowych (Financial Investigator, FI). Akredytacja ta daje funkcjonariuszowi możliwość nawiązywania bezpośredniego kontaktu z instytucjami finansowymi w celu uzyskania informacji istotnych dla trwających dochodzeń. Droga do kariery zawodowej dla funkcjonariuszy zajmujących się dochodzeniami

finansowymi opiera się na trzech tygodniowych kursach, obejmujących kurs podstawowy, kurs konfiskaty mienia i moduł dotyczący prania pieniędzy. Przewidziano także dodatkowe kursy dla funkcjonariuszy wywiadu terenowego, którzy posiadają szczególne możliwości śledcze w zakresie dochodzeń finansowych.

Podstawowa doktryna dochodzeniowa stanowi zatem podstawę nauczania problematyki dochodzeń karnych w całym programie PIP. Jak wspomniano wcześniej, doktryna stanowi zbiór zasad i procedur dla śledczych, według których należy prowadzić dochodzenie.

Na początku dochodzenia śledczy określa możliwe hipotezy oraz podejście dochodzeniowe, a następnie opracowuje strategię. Chciałbym tylko poruszyć kilka kwestii dotyczących tych strategii, aby zademonstrować podejście do kształcenia i jego znaczenie w walce z przestępczością, poparte badaniami naukowymi. Twierdzę, że zadbanie o fundamentalne kwestie stanowi podstawę każdego dochodzenia na jakimkolwiek szczeblu.

Strategia dochodzeniowa:

W pierwszej kolejności śledczy zdobywają wiedzę na temat strategii dochodzeniowej. Frazer (2008) stwierdza, że dochodzenia stanowią połączenie szeregu dowodów naukowych i technologicznych oraz danych wywiadowczych wspierających dochodzenia kryminalne. Prowadzenie dochodzeń wymaga uporządkowanej współpracy policyjnych zespołów dochodzeniowo-śledczych i szeregu specjalistów w celu zagwarantowania skutecznych wyników. W zeszłym tygodniu policja West Yorkshire na północy Anglii ogłosiła wspólnie z naukowcami Uniwersytetu w Sheffield najnowsze osiągnięcia w zakresie technik identyfikacji odcisków palców, pozwalających na ustalenie czy osoba, która pozostawiła odciski palców w miejscu przestępstwa pozostawiła je pod wpływem alkoholu lub narkotyków. W jednym z analizowanych przypadków badaczom i śledczym udało się ustalić, że odciski palców podejrzanego pochodzące z miejsca przestępstwa badanego 30 lat wcześniej wskazują na to, że podejrzany był wtedy pod wpływem alkoholu.

Można zatem podsumować, że śledczy zdobywają wiedzę na temat zasad prowadzenia śledztwa, na przykład zasady Locarda oraz jej znaczenia dla opracowywania lub eliminowania hipotez śledczych. Slajd pokazuje zasady wymiany przekazywane funkcjonariuszom policji, którzy muszą pamiętać o tym, że pozostawianie próbek może przebiegać w obie strony – dana osoba może pozostawić próbkę na miejscu, może też nastąpić zebranie próbki przez inną osobę, występuje także transfer wtórny. Jednocześnie funkcjonariusze nie mogą zapominać o tym, że brak dowodów nie stanowi dowodu nieobecności. Teorie te opierają się na znajomości rodzaju materialnych śladów i pozostałości branych pod uwagę w ramach śledztwa. Funkcjonariusze uczą się także praktycznych kwestii dotyczących odzyskiwania próbek biologicznych i fizycznych podczas czynności na miejscu zdarzenia. Warto też pamiętać, że umiejętności specjalistów w zakresie kryminalistyki opierają się w równej mierze na wyuczonych zachowaniach. W celu wypracowania praktyk pracy pomiędzy śledczymi i specjalistami w zakresie kryminalistyki, wszyscy studenci Uniwersytetu Lancashire mogą skorzystać z programu nauki w praktyce na ukończonej niedawno Akademii Kryminalistyki – Forensic Science Academy. Jednym z celów tej Akademii jest promowanie kultury i znaczenia podejścia do dochodzenia opartego na dowodach.

Strategia dochodzeniowa

Kluczowym elementem walki z przestępczością jest proces przeprowadzania przesłuchań. Pragnę poruszyć tę kwestię jako przykład kolejnego obszaru, który udało się rozwinąć dzięki ogromnemu wkładowi społeczności akademickiej. Bez względu na to, czy chodzi o reaktywne przesłuchanie ofiar lub świadków, czy też o proaktywną rozmowę z informatorami, przesłuchania stanowią kluczowy element strategii realizowanej przez wyższego rangą oficera dochodzeniowego. Jest to jeden z głównych wątków, pojawiający się we wszystkich szkoleniach policyjnych na poziomach od PIP1 do PIP3.

Szkolenia policyjne koncentrują się na przesłuchaniach w celu odkrycia prawdy, a nie dążenia do przyznania się przez osobę przesłuchiwaną. Filozofia ta jest istotną zmianą wpływającą na mentalność. Metody szkoleniowe związane z przesłuchaniami oparte są na akronimie PEACE, który rozwija się jako: przygotowanie i planowanie przed przesłuchaniem, zaangażowanie i wyjaśnienia, zaproszenie do przedstawienia wstępnej wersji wydarzeń, które może obejmować: kwestionowanie i wyjaśnienie, zamknięcie wraz z możliwością dodania lub wyjaśnienia niektórych elementów, a następnie proces oceny. Z mojego doświadczenia i obserwacji, szczególnie na pierwszym etapie szkolenia zawodowego wynika, że struktura ta zapewnia podstawowe ramy, na których mogą opierać się śledczy, jednak funkcjonariusze, którzy nie wykształcili wystarczająco umiejętności miękkich rygorystycznie trzymając się tych ram, tracą wiele możliwości, dzięki którym możliwe jest poprawienie przepływu informacji.

Pomimo tego, na etapie PIP2 następuje lepsze dopasowanie funkcjonariuszy do strategicznego podejścia do przesłuchiwania podejrzanych, uczestnicy mają także możliwość uczestniczenia w bardziej zaawansowanych kursach z zakresu techniki przesłuchań w ramach programu PIP. Szkolenie to zostało w znacznym stopniu oparte na badaniach akademickich, czego przykładem jest między innymi nauka prowadzenia przesłuchań w strategiczny sposób, poruszanie kwestii takich jak taktyczne korzyści wynikające ze zwiększenia obciążenia poznawczego podczas przesłuchania lub strategiczne przedstawianie dowodów. Wpływ środowiska akademickiego można dostrzec na tym slajdzie – widzimy na nim wytyczne dotyczące radzenia sobie z próbami oszustw w czasie przesłuchań z perspektywy oszusta i osoby je wykrywającej. Od samego początku śledczy mogą teraz wykorzystywać ważne badania dotyczące technik przeprowadzania przesłuchań i zwyczajów dostawcy i oszusta, a także działań, które śledczy powinien podjąć w ramach przepisów dotyczących ujawniania informacji.

Strategia danych biernych

Inną strategią dochodzeniową, którą poznają funkcjonariusze, jest strategia dostępu do danych biernych i ich gromadzenia. Według doniesień, Wielka Brytania posiada największą liczbę kamer przemysłowych (CCTV) i innych pasywnych źródeł danych na świecie. Wielokrotnie jednak krytykowano niski stopień wykorzystania danych z kamer przemysłowych w dochodzeniach i osobiście wierzę, że policja w Wielkiej Brytanii mogłaby skuteczniej zwalczać przestępczość, gdyby były dostępne lepsze szkolenia i gdyby przeznaczono dodatkowe środki na pozyskiwanie dowodów pochodzących z tego źródła. Jednakże w ważnych dochodzeniach śledczy określają zwykle strategię gromadzenia danych. Na tym slajdzie

widzimy, że Tilly (2007) wskazuje, że w przypadku 18% masowych przestępstw względem własności identyfikuje się bezpośredniego podejrzanego. Co ciekawe, z usług informatorów korzysta się w zaledwie 0,5% przypadków.

Strategia wywiadowcza

Strategie wywiadowcze mają kluczowe znaczenie w zwalczaniu przestępczości. Krajowy model wywiadu (National Intelligence Model) zapewnia znormalizowane podejście do gromadzenia, koordynacji i rozpowszechniania informacji wywiadowczych, które mogą być następnie zintegrowane ze wszystkimi siłami policyjnymi i organami ścigania. Jak widać na tym slajdzie, model działa na trzech poziomach:

Poziom 1. to dane wywiadowcze zbierane na szczeblu lokalnym; poziom 2. to dane wywiadowcze na poziomie poszczególnych jednostek i regionów, podczas gdy poziom 3. stanowią dane dotyczące poważnej i zorganizowanej przestępczości, w tym przestępczości krajowej i międzynarodowej. Zwalczanie przestępczości jest uzależnione od tego, w jaki sposób oceniane są informacje wywiadowcze, zarówno na poziomie strategicznym, jak i operacyjnym, w celu określenia profili problemów i ukierunkowania działań.

Śledczy zdobywają wiedzę na temat krajowego modelu wywiadu, który umożliwia przepływ informacji wywiadowczych i pozwala na podejmowanie decyzji w sprawie priorytetów dotyczących przestępczości i odpowiednich odpowiedzi taktycznych. Slajd, który widać obecnie przedstawia komplikacje wynikające z międzynarodowej skali przestępczości. Porównuje się mobilność ludności; w 1950 roku do Wielkiej Brytanii przybyło zaledwie dwadzieścia pięć milionów osób, podczas gdy obecnie radzimy sobie z miliardem osób wjeżdżających do kraju. Rosnąca mobilność transgraniczna ludzi oznacza dużą liczbę zabójstw, dochodzenia w sprawach poważnych przestępstw, a także konieczność prowadzenia dochodzeń w jednym lub kilku krajach. W szczególności dotyczy to tematu nadużyć finansowych i dochodzeń w sprawach przestępstw finansowych. Istnieje duże prawdopodobieństwo, że zespoły specjalistyczne działające w ramach Krajowej Agencji ds. Przestępczości (National Crime Agency) dysponują większą wiedzą i udzielą specjalistycznej pomocy jednostkom policji, ponieważ nie istnieje żadne formalne szkolenie w zakresie prowadzenia dochodzeń za granicą.

Jakakolwiek strategia wywiadowcza opiera się na zasadzie, że każdy kontakt pozostawia po sobie ślad, z tego powodu śledczy określa strategię, która obejmuje otwarte źródła, pasywne dane i tajne źródła danych oraz możliwości, które dają tego rodzaju dane. Żadna strategia wywiadowcza nie jest kompletna bez uwzględnienia całego wachlarza informacji wywiadowczych i informacji finansowych. Widoczny slajd przedstawia możliwości pozyskania informacji wywiadowczych na potrzeby dochodzenia dzięki starannie przemyślanej strategii wywiadowczej.

W Wielkiej Brytanii funkcjonariusze ds. wywiadu finansowego pracują w jednostkach wywiadowczych, wspierając wszelkie działania dochodzeniowe na wszystkich szczeblach.

Śledczy uczą się, że podejmowanie decyzji dotyczących wywiadu nie jest jedynie prostym, liniowym procesem; wymaga bowiem zestawiania i oceny dowodów oraz zebranych informacji w celu upewnienia się, że strategie dochodzeniowe zostały zakończone. Funkcjonariusze dowiadują się jednocześnie, że kluczowym narzędziem realizacji tego celu jest proces zgodny

z krajowym modelem decyzji (National Decision Model). Cykl ten stanowi podstawę szkolenia śledczego w Wielkiej Brytanii i zapewnia logiczne i uporządkowane podejście do podejmowania decyzji w pięciu etapach. Cykl ten jest wykorzystywany do podejmowania decyzji na odpowiednim szczeblu śledztwa, niezależnie od jego powagi i złożoności. Rozpoczyna się od gromadzenia informacji, identyfikacji luk i braków w zebranych danych, a następnie przechodzi do opracowania planu ich uzupełnienia, oceny ryzyka i opracowania strategii roboczej w drugim etapie, po którym następuje analiza uprawnień, obowiązujących zasad i procedur. Na następnym etapie bierze się pod uwagę opcje i nieprzewidziane okoliczności, a podejmuje się działania z okresem przeglądu. Wszystkie te działania odbywają się cyklicznie, a u ich źródła znajdują się misja i wartości.

Wcześniej odniosłem się także do znaczenia ram prawnych i podejścia osoby prowadzącej dochodzenie oraz do ich konsekwencji wobec procesu decyzyjnego.

Profesjonalizacja policji w Wielkiej Brytanii

Pojęcie to odnosi się do szeroko zakrojonego programu reform opartego na utworzeniu College of Policing. Ambicją nowej wyższej szkoły dla policjantów jest to, aby zawodowe osiągnięcia akademickie każdego funkcjonariusza były oficjalnie uznane. Ilość kursów, w których wziąłem udział przez cały okres mojej służby w policji, a które nie zostały formalnie uznane za kwalifikacje, skłania mnie do refleksji nad zmarnowanymi możliwościami; jednak nie jest to problem, z którym będziemy mieli do czynienia w przyszłości. W połączeniu z programem ramowym zapewnienia jakości kształcenia funkcjonariuszy (Police Educational Quality Framework), w przyszłości brytyjscy policjanci będą zobowiązani do zdobywania odpowiedniego wykształcenia na każdym szczeblu służby, od posterunkowego, który będzie wymagał zdobycia 6. poziomu wykształcenia odpowiadającego stopniowi licencjata, aż do stopnia nadinspektora wymagającego kwalifikacji na poziomie magistra, a także Komendanta Głównego, którego stanowisko będzie się wiązało z koniecznością zdobycia odpowiednika doktoratu zawodowego – 8. poziomu wykształcenia. Zakres ten daje organizacji możliwość dalszego włączania do programu pracy policji działań opartych na wiedzy dzięki prowadzonym badaniom oraz kształceniu pracowników, którzy będą w stanie sprostać przyszłym wyzwaniom dzięki wiedzy i umiejętnościom wykraczającym poza tradycyjne metody policyjne.

Przyszłość umożliwi zatem znacznie ściślejszą integrację przedsiębiorstw, środowisk akademickich i służb policyjnych w celu wspólnej pracy na rzecz walki z przestępczością, policjanci zaś będą odpowiednio przygotowani i wyszkoleni do stawiania czoła wyzwaniom. Jednym z głównych celów jest przyciągnięcie szerszego grona kandydatów na funkcjonariuszy poprzez poszerzenie tradycyjnych kanałów dostępu do organizacji oraz dostrzeganie talentów w różnych branżach.

Rola szkolnictwa wyższego i prowadzenia badań dotyczących działalności policji w Wielkiej Brytanii stale nabiera coraz większego znaczenia, obecnie w całym kraju działają ośrodki badawcze skupiające się na całym spektrum problemów i kwestii związanych z działaniami policji. Na ekranie widzą państwo teraz zdjęcie jednego z kampusów na Uniwersytecie w Central Lancashire, gdzie pracuję. Obecnie dysponujemy zespołami naukowców, pracującymi nad definiowaniem, identyfikowaniem i reagowaniem na zagrożenia przez policję, a także

kwestiami takimi jak dokonywanie szczegółowej oceny ryzyka przemocy domowej, przemocy w rodzinie i współpracy z policją oraz tego, czy wieloagencyjne węzły ochrony (MASH) stanowią skuteczny sposób ochrony osób w trudnej sytuacji. W całym kraju trwają jednak prace nad rozwojem działań policyjnych opartych na wiedzy oraz nad projektami badawczymi.

Na koniec chciałbym nawiązać do oferty Uniwersytetu w Central Lancashire. Oferujemy programy studiów magisterskich w zakresie dochodzeń finansowych, dochodzeń w sprawach cyberprzestępczości, praktyk zawodowych i wczesnej interwencji, zwalczania terroryzmu i dochodzeń karnych. Dzięki temu przyciągamy wielu studentów zajmujących się biznesem, a także przedstawicieli środowiska akademickiego. Obecnie na naszej uczelni można spotkać studentów z różnych dziedzin biznesu, w tym adwokata z Międzynarodowego Trybunału Karnego, przedstawicieli Barclays Bank i innych instytucji finansowych uczestniczących obecnie w programie studiów magisterskich dla śledczych finansowych.

Uniwersytet w Central Lancashire posiada dobrze ugruntowany program studiów licencjackich i magisterskich, który cieszy się prawdziwie międzynarodowym uznaniem. Obejmuje on szeroki zakres preferencji edukacyjnych, w tym między innymi możliwość nauki zdalnej. Pomimo tego, że moduł cieszy się dużą popularnością, działa z powodzeniem dzięki różnorodności uczestniczących w nim przedstawicieli świata biznesu, środowisk akademickich i organów ścigania.

Przyszłe aspiracje obejmują kursy rachunkowości kryminalistycznej, umiejętności kluczowej dla śledztw związanych z nadużyciami finansowymi oraz dla dochodzeń finansowych.

Podsumowując, w Wielkiej Brytanii stale rozwijają się powiązania między badaniami akademickimi i metodami działalności operacyjnej policji. Dzieje się tak pomimo faktu, że na poziomie operacyjnym funkcjonariusze liniowi nie korzystają jeszcze z refleksyjnego podejścia opartego na wiedzy, a szkolenia policyjne w dalszym ciągu mogą pełnić lepszą rolę w tym zakresie. Przyszli liderzy wyższego szczebla w ramach organizacji mogą mieć mniejsze doświadczenie operacyjne, prowadząc dochodzenia w sprawach karnych, jednak dzięki przyciągnięciu większej puli talentów oraz skorzystania z doświadczenia akademickiego, do tych liderów będzie należała misja dalszej zmiany kultury i przekonywania funkcjonariuszy do pracy opartej na wiedzy.

PROTECTION OF THE FINANCIAL INTERESTS OF THE EU – COMMON OBLIGATIONS AND CHALLENGES

International Conference
Katowice, 23-27 October 2017

OLAF
EUROPEAN ANTI-FRAUD OFFICE

POLICJA

POLICJA

SZKOŁA POLICJI KATOWICE

This conference is supported by the European Union Programme Hercule III (2014-2020).
This programme is implemented by the European Commission. It was established to promote activities in the field of the protection of the financial interests of the European Union.

Szkoła Policji
w Katowicach

Komenda Wojewódzka Policji
w Opolu

Komenda Wojewódzka Policji
w Katowicach

Projekt współfinansowany przez Program Unii Europejskiej Hercule III (2014-2020).
Program jest realizowany przez Komisję Europejską i został ustanowiony w celu promowania działalności w dziedzinie ochrony interesów finansowych Unii Europejskiej.

EUROPEAN ANTI-FRAUD OFFICE

ISBN 978-83-934380-6-8