Bundeskriminalamt

Edited by

Ursula Töttel
Gergana Bulanova-Hristova
Gerhard Flach

Research Conferences on Organised Crime at the Bundeskriminalamt in Germany

Vol. III

Transnational Organised Crime

2013 – 2015

Research Conferences on Organised Crime
2013 – 2015

Bundeskriminalamt

Edited by

Ursula Töttel
Gergana Bulanova-Hristova
Gerhard Flach

Research Conferences on Organised Crime at the Bundeskriminalamt in Germany

Vol. III

Transnational Organised Crime

2013 – 2015

BKA

Foreword

Money laundering, drug trafficking, trafficking in human beings, migrant smuggling, arms trafficking, vehicle trafficking and receiving of stolen luxury goods as well as organised property crime and cybercrime are now a business worth billions and – along with international terrorism – are among the major security challenges of our time. The liberalisation of the world economy and rapidly progressing technological developments benefit not only the economic sector, but also organised crime throughout the world. Even at a time with a growing number of crises – such as those associated with the rising number of refugees or terrorist attacks worldwide – the threat posed by organised crime should not be underestimated.

Organised crime is a global phenomenon that does not stop at borders or fail to penetrate certain sectors. It is generally associated with corruption, violence, exploitation and infiltration of legal structures, and it affects the life and well-being of thousands of people. In contrast to terrorist attacks, the general public often only becomes aware of organised crime in subtler ways. The criminal actions of human traffickers and migrant smugglers (from the Balkans, for example), of drug cartels from Latin America or of corrupt local politicians who provide mafia organisations with lucrative government contracts do not come close to provoking the degree of existential fear that results from terrorist acts of violence. Nevertheless, the potential for damage caused by often violent OC offences committed to obtain items of economic value or political influence is great, and the risk of becoming a victim of organised crime is no less real. The activities of organised criminals do not become clearly visible to the public until large segments of the population are victimised, for example due to dwelling burglary by organised criminals or the theft of credit card data and identities on the internet.

Organised crime continues to be a serious problem for Germany – a trend confirmed by the 2014 National Situation Report on organised crime: As in 2013, drug crime along with property and economic crime are among the main fields of OC activity.[1] In addition, an increase in migrant smuggling is evident. In 2014, there were investigations of 35 OC groups (2013: 29) working in the field of migrant smuggling[2]; in most cases Syrian refugees were smuggled. However, these figures only reflect recorded crime. Organised crime is not limited by borders, as indicated by the fact that two-thirds of the

---

[1] Cf. the 2014 national situation report on organised crime: BKA, Organisierte Kriminalität Bundeslagebild 2014, p. 7, http://www.bka.de/DE/ThemenABisZ/Deliktsbereiche/Organisierte Kriminalitaet/Lagebilder/lagebilder__node.html?__nnn=true (11. 12. 2015).

[2] Ibid., p. 25.

suspects come from outside Germany and that international links exist in 80% of OC investigative proceedings

Organised crime is internationally networked, operates in a highly conspiratorial manner and causes considerable damage. According to estimates by the United Nations among others, today the business dealings of transnational organised crime generate an annual turnover of several hundred billion US dollars. Besides this, the internet offers criminal groups a wide variety of possibilities, serving as an instrument of crime and as a virtual crime scene. At the same time, cybercrime is considered to be a "low risk – high profit" business made even more attractive by the "crime as a service" model, which makes it easy to purchase criminal services.

Are we in an optimal position to fight organised crime in Germany and in Europe? We are working very hard – and successfully – on expanding and adapting our law enforcement strategies and instruments. Our police work is effectively networked, Europe-wide through EUROPOL and worldwide through INTERPOL, which enables us to join together in the battle against organised groups that operate across national borders. In order to benefit even more from combining our strength in an optimal manner, at the Bundeskriminalamt Germany, for example, an organised crime coordination unit (KOST-OK) has been set up to ensure a structured exchange of information about OC developments at federal and state level. The unit also serves as a central point of contact for international police cooperation and, at the same time, it is intended to provide impetus for the setting of priorities at EUROPOL. In addition to structural optimisation, the Bundeskriminalamt Germany employs a project-oriented approach to analysis and law enforcement aimed at organised crime and at structures similar to those of organised crime. In doing so, we rely on the principle of intensive information exchange across organisational boundaries in order to arrive at the most comprehensive possible analysis of the potential threat posed by various groups and in order to initiate joint investigations. Considering the highly dynamic nature of organised crime, there are obvious advantages to taking a flexible, time-limited approach aimed at areas where criminal activity is currently concentrated. Furthermore, we will work continually to optimise these structures. A successful battle against a highly complex phenomenon like organised crime should be based on a solid analytical foundation – a realisation that is not new but repeatedly proves to be significant. This is why the Bundeskriminalamt relies on close collaboration between practical police work and research in the fields of criminalistics and criminology. The focus is on both technical and social-scientific studies, which serve to collect information that goes beyond the police channels, to analyse the causes and characteristics of new forms of criminal activity and modi operandi, to prepare assessments of various relationships, to shed light

on the "dark fields" of crime by employing scientific methods of data collection, and to adapt action recommendations to changing security requirements.

One result of this cooperation between research and practical police work, which is traditional for the Bundeskriminalamt, is the – now third – volume with contributions from the BKA research conferences held from 2013 through 2015. The conference topics "Organised Crime and the Internet", "The Different Faces of Organised Crime" and „Countering International Organised Crime Groups – Challenges and Opportunities" were chosen as priority areas because they are important for work in the field of law enforcement and also in the field of science. Like the first two volumes, this collection of contributions again aims at providing a broad expert audience from different countries with insight into the current work and research results presented at the BKA's annual organised crime research conferences. This publication is also intended to emphasise the importance of interconnecting operational and scientific expertise and to promote expanded cooperation with further partners at national and international level.

Holger Münch, President of the Bundeskriminalamt

Translation of the German foreword

Vorwort

Geldwäsche, Drogenschmuggel, Menschenhandel, Schleusung, Waffenhandel, Kraftfahrzeugverschiebung und Hehlerei von Luxuswaren, aber auch organisiert begangene Eigentumskriminalität und Cybercrime sind Milliardengeschäfte und gehören – neben dem internationalen Terrorismus – zu den zentralen Sicherheitsherausforderungen der Gegenwart. Die Liberalisierung der Weltwirtschaft und rasch fortschreitende technologische Entwicklungen bringen nicht nur Vorteile für den Wirtschaftssektor mit sich, sondern auch für das organisierte Verbrechen weltweit. Auch in Zeiten zunehmender Krisenlagen – wie im Zusammenhang mit steigenden Flüchtlingszahlen oder Terroranschlägen weltweit – dürfen die Bedrohungen, die von der Organisierten Kriminalität (OK) ausgehen, nicht unterschätzt werden.

OK ist ein globales Phänomen, das weder an Grenzen noch vor Branchen haltmacht. Sie geht in der Regel mit Korruption, Gewalt, Ausbeutung und Unterwanderung legaler Strukturen einher und betrifft das Leben und Wohlergehen Tausender Menschen. Im Unterschied zu terroristischen Anschlägen manifestiert sich das organisierte Verbrechen für die breite Öffentlichkeit vielfach eher subtil. Das kriminelle Handeln von Menschenhändlern und Schleusern, beispielsweise vom Balkan, von Drogenkartellen aus Lateinamerika oder von korrupten Kommunalpolitikern, die Mafia-Organisationen mit lukrativen Staatsaufträgen versorgen, ruft bei Weitem nicht so erhebliche existenzielle Ängste hervor wie terroristische Gewalttaten. Dennoch ist das Schadenspotenzial der organisierten, häufig gewalttätigen Kriminalitätsbegehung zur Erlangung wirtschaftlicher Werte oder politischen Einflusses hoch und das Risiko, Opfer der OK zu werden, nicht weniger real. Das Agieren des organisierten Verbrechens wird der Öffentlichkeit erst dann deutlich sichtbar, wenn breite Teile der Bevölkerung selbst Opfer werden, z. B. bei organisiert begangenen Wohnungseinbrüchen oder beim Kreditkartendaten- und Identitätsdiebstahl im Internet.

Für Deutschland bleibt die OK ein ernstes Problem – ein Trend, der auch im Bundeslagebild 2014 Bestätigung findet: Rauschgift- sowie Eigentums- und Wirtschaftskriminalität gehören, wie schon 2013, zu den Hauptaktivitätsfeldern der OK.[1] Zudem ist ein Anstieg der Schleusungskriminalität erkennbar. 2014 wurde gegen 35 OK-Gruppen (2013: 29) im Bereich der Schleusungskriminalität ermittelt,[2] geschleust wurden in den meisten Fällen syrische

---

[1] Vgl. BKA, Organisierte Kriminalität Bundeslagebild 2014, S. 7, http://www.bka.de/DE/ThemenABisZ/Deliktsbereiche/OrganisierteKriminalitaet/Lagebilder/lagebilder__node.html?__nnn=true (11. 12. 2015).

[2] Ebd., S. 25.

Staatsangehörige. Diese Zahlen bilden allerdings lediglich das Hellfeld ab. Dass die OK keine Staatsgrenzen kennt, zeigt die Tatsache, dass zwei Drittel der Tatverdächtigen aus dem Ausland stammen und insgesamt 80 Prozent der OK-Ermittlungsverfahren internationale Bezüge aufweisen.

Die OK ist international vernetzt, agiert äußerst konspirativ und verursacht erhebliche Schäden. Nach Schätzungen u. a. der Vereinten Nationen werden inzwischen jährlich mehrere Hundert Milliarden US-Dollar bei Geschäften der transnationalen organisierten Kriminalität umgesetzt. Hinzu kommt, dass das Internet den Tätergruppierungen vielfältige Möglichkeiten als Tatmittel und als virtueller Tatort bietet. Dabei gilt Cybercrime als ein „*low risk – high profit*"-Geschäft, dessen „Attraktivität" durch das „*crime as a service*"-Modell des einfachen Ankaufs krimineller Dienstleistungen gesteigert wird.

Sind wir in Deutschland, sind wir in Europa für die Bekämpfung der OK optimal aufgestellt? Wir arbeiten mit Hochdruck an Ausbau und Anpassung der Strafverfolgungsstrategien und -instrumente – und das mit Erfolg. Wir sind mit EUROPOL europaweit und mit INTERPOL weltweit polizeilich gut vernetzt und in der Lage, gemeinsam transnational organisierte Gruppen zu bekämpfen. Um noch mehr von einer optimalen Kräftebündelung profitieren zu können, wurde beispielsweise im BKA eine Koordinierungsstelle OK (KOST-OK) eingerichtet, die den strukturierten Erkenntnisaustausch zu den OK-Entwicklungen in Bund und Ländern gewährleisten wird. Die Stelle dient auch als zentraler Ansprechpartner für die internationale polizeiliche Zusammenarbeit und soll zugleich Impulsgeber für Schwerpunktsetzungen bei EUROPOL sein. Neben den strukturellen Optimierungen implementiert das BKA einen projektorientierten Ansatz zur Auswertung und Strafverfolgung von OK und OK-ähnlichen Strukturen. Wir setzen dabei auf das Prinzip des engen Informationsaustauschs über Organisationsgrenzen hinweg, um eine möglichst umfassende Auswertung des Gefährdungspotenzials unterschiedlicher Gruppen zu erreichen und gemeinsame Ermittlungen einzuleiten. Die Vorteile dieses flexiblen und zeitlich befristeten Projektansatzes, der sich an aktuellen Schwerpunkten orientiert, liegen angesichts der hochdynamischen Natur der OK auf der Hand. Wir werden aber auch weiterhin kontinuierlich an einer Optimierung dieser Strukturen arbeiten. Die erfolgreiche Bekämpfung eines hochkomplexen Phänomens wie der OK sollte auf einem soliden analytischen Fundament basieren – das ist keine neue, jedoch immer wieder bedeutsame Erkenntnis. Daher setzt das BKA auf die enge Zusammenarbeit zwischen polizeilicher Praxis und kriminalistisch-kriminologischer Forschung. Im Mittelpunkt stehen dabei sowohl technische als auch sozialwissenschaftliche Untersuchungen, die dazu dienen, Informationen über die polizeilichen Kanäle hinaus zu erheben, Ursachen und Ausprägungen neuartiger Tatbilder und Vorgehensweisen zu analysieren, Bewertungen unterschiedlicher Zusammenhän-

ge zu erstellen, „Dunkelfelder" anhand wissenschaftlicher Erhebungsmethoden aufzuhellen und Handlungsempfehlungen an sich ändernde Sicherheitsanforderungen anzupassen.

Ein Ergebnis dieser für das BKA traditionellen Zusammenarbeit zwischen Forschung und Polizeipraxis ist der nunmehr dritte Band mit Beiträgen der Forschungskonferenzen der Jahre 2013 bis einschließlich 2015. Mit den Tagungsthemen *„Organised Crime and the Internet"*, *„The Different Faces of Organised Crime"* und *„Countering International Organised Crime Groups – Challenges and Opportunities"* wurden Schwerpunkte ausgewählt, die sowohl für die Strafverfolgung als auch für die Wissenschaft wichtige Arbeitsschwerpunkte bilden. Wie die beiden ersten Bände zielt auch dieser Sammelband darauf ab, einem breiten internationalen Fachpublikum Einblick in die aktuellen Aufgaben und Forschungsergebnisse, die auf den jährlichen OK-Forschungskonferenzen des BKA präsentiert wurden, zu gewähren. Mit dieser Veröffentlichung wollen wir zudem die Bedeutung der Verzahnung operativer und wissenschaftlicher Expertise unterstreichen und für den Ausbau der Zusammenarbeit mit weiteren Partnern auf nationaler und internationaler Ebene werben.

Holger Münch, Präsident des Bundeskriminalamts

Table of Contents
Inhaltsverzeichnis

Part IV

Deutscher Teil
Part V

Part VI

English Part
Part I

EU Project "Research Network on Organised Crime" 2010–2016[1]

Cooperation at the international level, and especially the European level, is becoming increasingly important in the field of security, and this is also true in the field of police research. At the BKA this was the basis for an idea: to promote Europe-wide cooperation between academics and practitioners from law enforcement agencies for the purpose of combating organised crime and to establish a forum that facilitates international exchange among those involved in such work. Together with research centres in Great Britain, the Netherlands and Sweden, the "OC Research Network" was founded. The activities of the Network received financial support from the EU from 2010 to 2016.

1   EU Project "Research Network on Organised Crime"

Within the framework of the Internal Security (ISEC) programme "Prevention of and Fight against Crime" – Framework Partnerships and together with research institutions in other countries, the Bundeskriminalamt requested funds for the EU project "Research Network on Organised Crime" (March 2010 – February 2013). Starting in 2010, the EU co-financed 70 percent of the project. The project included holding two working meetings with the project partners each year, organising an annual OC research conference, and publishing two collections of contributions made by the speakers at the research conferences. The objectives of the project were to identify current topics and methods in the field of OC research and to exchange information about research programmes and projects. Regular Network meetings were to be held during which areas of organised crime were examined and selected priority topics were discussed. The research conferences aimed at providing an overview of the research situation and areas of emphasis as well as information about the crime situation and strategies to combat crime in European countries. The overall aim of the project was to intensify the exchange of information and ideas about organised crime among persons active in the academic and law enforcement fields at both national and international level.

An application was submitted for an EU follow-up project within the framework of the ISEC programme "Prevention of and Fight against Crime 2007–2013, Action Grants 2011, General call for proposals". The European Commission again acknowledged the importance of the Network and the research

---

[1] Parts of the document were adopted from "Research Network on Organised Crime 2010–2013 – Bericht über ein EU-Projekt" by Ursula Töttel and Gerhard Flach, "Kriminalistik", 6/2014.

conferences and approved the funding request. Compared to the original project, in the follow-up project some of the changes involved a (larger) number of participants, recruitment of speakers – also from outside the EU – and the subject matter dealt with at the annual research conferences. The follow-up project for which funding was requested – "Research Network on Organised Crime 2013–2016" – received even more EU support – 89.5%. It ran from March 2013 until the end of February 2016.

2 Development of the Project Idea

2.1 The search for cooperation partners

In view of the increasing cross-border activity of OC groups, it was considered necessary to take an international approach, not only to OC suppression but also to OC research. Steps to realise this idea were taken in 2007, when representatives of the BKA research and advisory unit on organised and economic crime (Forschungs- und Beratungsstelle für Organisierte und Wirtschaftskriminalität) made initial contact with the Home Office in London. This was followed by a first exchange of information about OC research projects in London. In 2008 contact was established with potential partners in Belgium and the Netherlands. The decisive factor when choosing institutions to contact was whether they were conducting social science research in the field of organised crime. Cooperation with government offices was sought. Closer examination revealed that, with regard to research involving criminology and criminal investigation in Europe, the BKA plays a special role, i. e. comparable government research facilities are generally associated with ministries – and not directly with the police. As a consequence, the search for potential partners was aimed at institutions outside the realm of police agencies.

2.2 Establishment of an OC research network

As a result of these initial contacts, in 2008 the "Crime Research Development Unit" of the Home Office in London, the "Research and Documentation Centre" (WODC) of the Ministry of Justice in The Hague and the Dutch Police Academy in Apeldoorn joined together to found the OC Research Network. As proposed by the Netherlands, it was decided to establish a network with a manageable number of participants in order to ensure effectiveness. Important changes occurred in 2010: The Dutch Police Academy left the Network and the "Swedish National Council for Crime Prevention" (Brå), Stockholm, which is subordinate to Sweden's Ministry of Justice, joined the Net-

work. The members of the Swedish research unit could not apply for any EU support because they joined the Network later. The makeup of the Network has not changed since then.

The first OC research conference was held in Frankfurt in November 2008. However, at this time it was not yet clear if further conferences would be held and if the Network would continue to exist.

3 Research Conferences and Network Meetings

3.1 Participants and organisation of the conferences

From 2008 to 2015, the Bundeskriminalamt hosted eight international OC research conferences in Frankfurt am Main, Wiesbaden, Niedernhausen and Mainz. The conferences facilitated the establishment of a comprehensive overview of the situation with regard to OC research and suppression in numerous European countries. These conferences provided a forum for a cross-border exchange of ideas and information by scholars and police practitioners regarding subjects and issues such as currently applied and conceivable alternative types of field access in the case of empirical research projects and the application of scientific findings to practical situations. They also provided insight into police strategies as well as into special aspects of, and difficulties posed by, law enforcement. Scholars and experts from law enforcement authorities in Albania, Austria, Belgium, Bulgaria, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Great Britain, Greece, Hungary, Italy, the Netherlands, Norway, Poland, Slovenia, Spain, Sweden, Switzerland, Turkey and the United States spoke at the conferences about their research activities or the current situation in their own country with regard to criminality and crime fighting. Europol and Interpol representatives also participated.

The conferences were organised on a geographical basis. The subjects included OC research and the situation in the countries bordering Germany (2008), in southeastern Europe (2009), in southwestern Europe (2010), in western Europe (Great Britain, Netherlands, 2011) and in northern Europe (2012). The conferences from 2013 to 2015 were organised on the basis of crime phenomena. The subjects chosen were organised crime and cybercrime (2013), the varying faces of organised crime (2014), and international OC groups (2015).

At each of these two-day conferences, seven or eight speakers talked about the special situation in their own countries or about their views on selected aspects of crime. The Network's partner institutions worked together to choose the speakers.

3.2   Objectives of the network meetings

The OC research network serves to intensify direct contacts between government research institutions and permits a coordinated assessment of development trends in science and law enforcement. In addition to working-level contacts for various reasons, each year there were two meetings of the participating institutions, meetings that were also useful for joint preparation of the OC research conferences. Information about current and planned research projects was exchanged along with other types of information – for example about threat assessments, situation assessments and approaches to crime fighting – as well as information from or about conferences or other relevant meetings and events.

4   Implementation of the Project

4.1   Cooperation with the project partners

When the project was carried out, it could be seen that a realistic timetable and advance determination of responsibilities and tasks within the framework of the joint project are meaningful and helpful. The first meetings and consultations, which were still quite formal and initially concentrated on carrying out a successful EU project, led to trustful and uncomplicated cooperation between the partner institutions that progressed beyond implementation of the activities.

In any case it was necessary for the BKA, as the institution heading the project, to take the initiative for each of the planned activities. When meetings were held, coordination was facilitated by keeping a written record of the work packages as well as other arrangements agreed upon. Conference calls proved to be valuable for ensuring information exchange among the network partners between the two conferences held each year. Continuity of staffing in the Network was beneficial.

Another aspect that should not be underestimated is the large amount of detail work for conference preparation and book publication as well as the process of coordination with research organisations in the other three European countries that was required for all project activities.

4.2   Experience gained from, and results of, the project work

It should be emphasised at this point that the assistance provided by the BKA section for EU-supported projects ("EU-geförderte Projekte"), which is part of the International Coordination Division, was highly beneficial for the en-

tire process. This section assists with applying for and carrying out EU projects, and a "financial manager"[2] for each project carried out within the framework of the ISEC programme is assigned to the project implementer.

During the course of the project, contacts were developed with German and other European universities, police colleges, and other institutions that conduct research in the field of organised crime. Representatives of research institutions, law enforcement agencies, public prosecutors' offices and international organisations spoke at the conferences. With a view to choosing subject matter for individual meetings, ideas and topics proposed by participants were continually recorded and discussed by the Network partners when planning subsequent meetings.

The publications provide an overview of the research situation in European countries, and the books as well as abstracts of the presentations are available through the BKA website.[3] The first book published, "Research Conferences on Organised Crime at the Bundeskriminalamt in Germany 2008–2010", appeared in October 2011.[4] The second publication about the conferences from 2009 to 2012 appeared in September 2013.[5] In addition, joint contributions by members of the OC Research Network were published.[6]

In cooperation with two research organisations from the Network, in March 2013 an international research project on the subject of organised crime and

---

[2] The financial manager is responsible for the handling of finances vis-à-vis the European Commission. This includes budgeting, defining appropriate cost structures, and calculation of services rendered.

[3] Information in German about the OC research conferences is available under http://www.bka.de/DE/ThemenABisZ/Forschung/OK-Forschungskonferenzen/ok-forschungs-konferenzen__node.html?__nnn=true and in English under http://www.bka.de/nn_195376/EN/SubjectsAZ/Research/OrganisedCrimeResearch/organisedCrimeResearch__node.html?__nnn=true.

[4] Töttel, Ursula, Büchler, Heinz, 2011. Research Conferences on Organised Crime at the Bundeskriminalamt in Germany 2008–2010, Polizei + Forschung Band 43 under http://www.bka.de/nn_193482/DE/Publikationen/Publikationsreihen/01PolizeiUndForschung/01PolizeiUndForschung__node.html?__nnn=true.

[5] Töttel, Ursula, Bulanova-Hristova, Gergana, Büchler, Heinz, 2013. Research Conferences on Organised Crime at the Bundeskriminalamt in Germany (Vol. II) – Organised Crime – Research and Practice in Western and Northern Europe, 2011–2012, Polizei + Forschung Band 45 under http://www.bka.de/nn_193482/DE/Publikationen/Publikationsreihen/01PolizeiUndForschung/01PolizeiUndForschung__node.html?__nnn=true.

[6] Several articles about human trafficking were published in 2011 in: Trends in Organized Crime: Special Issue: Human Trafficking, Vol. 14, 2011, http://www.springerlink.com/content/1084-4791/14/2-3/ (link to the freely accessible articles). A conference report about the 4th OC Research Conference in November 2011 was published in 2012: Töttel, Ursula, Bulanova-Hristova, Gergana, Kleemans, Edward, 2012. Trends in Organised Crime, Vol. 15, Research on organized crime in Western Europe – 4th research conference "OC research in Western European states" in Wiesbaden, http://link.springer.com/article/10.1007/s12117-012-9176-y#page-1.

cybercrime was initiated, and a proposal for funding within the framework of the European Commission's ISEC General Call for Proposals was submitted, with approval being granted in December 2013. The two-year project, "Cyber-OC – Scope and manifestations in selected EU member states", ran from April 2014 to March 2016.

5   Further Funding Possibilities for the Activities

In the past, the European Commission provided six funding instruments in the area of internal security. As of 1 January 2014, these were reduced to two instruments – the Asylum and Migration Fund (AMF) and the Internal Security Fund (ISF) 2014 – 2020.[7] This means that the ISEC programme, which served as the framework for the EU project described here, is being replaced by the ISF.

There is currently no European Commission Call on which an application for another follow-up project could be based, but perhaps future Calls can serve as a suitable basis.

6   Conclusions

Implementation of the EU project "Research Network on Organised Crime" created added value for OC Research Network participants, both professionally and personally. On the one hand, there was an exchange of the most recent knowledge regarding developments and research activities as well as information about law enforcement in the field of organised crime, while on the other hand, years of regular meetings involving staff from the respective research institutions strengthened cooperation. Participants in the organised crime conferences also profited from the exchange of experience that occurred in connection with the speeches and contacts at the conferences. The project publications made the results of the conferences available to a wide audience of professionals in this field. We intend to maintain the OC Research Network and to hold conferences in the future as well.

---

[7] See also: European Commission under: http://ec.europa.eu/dgs/home-affairs/financing/fundings/funding-home-affairs-beyond-2013/index_en.htm.

Description of the Research Partnering Institutions

Research and Advisory Unit for Organised Crime, Economic Crime and Crime Prevention of the Bundeskriminalamt (BKA), Germany

Forming part of the Criminalistic-Criminological Research Group (KI 1) of the BKA, the Research and Advisory Unit for Organised Crime, Economic Crime and Crime Prevention (KI 14) is the leading organised crime research unit of the German police. KI 1 is organised into the following research units.

– Terrorism/Extremism Research Unit (German acronym: FTE)

– Police Crime Statistics Research Unit (PKS), crime statistics-related/criminological analyses, research on unreported/undetected crime

– Operational Case Analysis (OCA), Research Unit for Violent Crime, Juvenile Delinquency

– Research and Advisory Unit for Organised Crime, Economic Crime and Crime Prevention

– Advisory Unit for Legal Matters and Legal Affairs

– Research and Advisory Unit for Cyber Crime

According to § 2 of the BKA Law it is the responsibility of the BKA to support the federal and state police in researching and answering questions related to police methods and approaches as well as phenomenological issues of crime suppression. The Research Unit for OC, Economic Crime and Crime Prevention is staffed by police practitioners and researchers operating at the interface between science and practice. Working in an interdisciplinary fashion and using scientific methodologies, the unit is tasked with resolving policing issues and pursuing the (further) development of implementation concepts. The process places emphasis on close coordination with users and clients. Section KI 14 carries out research and advisory tasks in the fields of organised crime, human trafficking and smuggling, as well as economic and financial crime and crime prevention.

Our work at present focuses on the following subjects, for which research projects were completed in 2015 or are currently being carried out:

– Im October 2015 the study: **„Compliance systems and and their effects on combatting and prevention of offences in the fields of economic crime and corruption"** (Compliance-Systeme und ihre Auswirkungen auf die Verfolgung und Verhütung von Straftaten der Wirtschaftskriminalität und Korruption) was published. It presents the results of an empirical study that considers the extent to which compliance systems influence the completion of tasks by law enforcement agencies in cases of economic crime and corruption as well as communication between companies and law enforcement agencies.

– The results of a secondary analysis at the Bundeskriminalamt conducted on the subject **„Economic and industrial espionage – an analysis of the current state of research"** (Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes) were published in October 2015 as well.

– In the current project, **„Pharmaceutical Crime 2"** (Arzneimittelkriminalität 2), situations are analysed, law enforcement deficiencies in the field of pharmaceutical crime are identified, and recommendations for action to correct these deficiencies are made. This is a follow-up to the project „Pharmaceutical Crime – A Growing Market" (Arzneimittelkriminalität – ein Wachstumsmarkt) published by the BKA in 2007. Completion of the study is expected in 2016.

– In addition, Section KI 14 and its project partners Research and Documentation Centre (WODC), The Hague, and Swedish National Council for Crime Prevention (Brå), Stockholm, are carrying out the EU-financed project **„Cyber OC – Scope and manifestations in selected EU member states"**, completion of which is expected by 1 April 2016.

Besides this, the Research Unit provides assistance as an associate partner for a number of ongoing projects in the context of security research at national level. These are the following collaborative projects, which consider various aspects of organised and economic crime and are supported by Germany's Federal Ministry of Education and Research (BMBF):[1]

---

[1] The website of the VdI association provides an overview of current research projects included in the programme „Research for civil security" (Forschung für die zivile Sicherheit): http://www.vditz.de/forschungsfoerderung/sicherheitsforschung/laufende-forschungsprojekte-im-ueberblick/.

- **Effects of liberalisation of electronic commerce in Europe on the phenomenon of pharmaceutical crime** (Auswirkungen der Liberalisierung des Internethandels in Europa auf den Phänomenbereich der Arzneimittelkriminalität – ALPhA),

- **Prevention and intervention in the case of human trafficking for sexual exploitation – A multidisciplinary and cross-institutional perspective** (Prävention und Intervention bei Menschenhandel zum Zweck sexueller Ausbeutung – Eine multidisziplinäre und institutionsübergreifende Perspektive – PrIMsA),

- **Prevention of capital market offences and risks of money laundering** (Prävention von Kapitalmarktdelikten und Risiken der Geldwäsche – PKG),

- **Risk management of corruption from the perspective of companies, local communities and the police** (Risikomanagement der Korruption aus der Perspektive von Unternehmen, Kommunen und Polizei – RIKO),

- **Procedures to shed light on undetected crime as a basis for crime fighting and prevention using ancient cultural objects as an example** (Verfahren zur Erhellung des Dunkelfeldes als Grundlage für Kriminalitätsbekämpfung und -prävention am Beispiel antiker Kulturgüter – Illicid),

- **Economic and industrial espionage in Germany and Europe** (Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa – WISKOS).

Organised and Cyber Crime Research & Analysis of the Home Office, United Kingdom

Organised and Cyber Crime Research & Analysis (OCCRA) is a team of social researchers, operational researchers and economists working within the Home Office. The Home Office is the lead government department for immigration and passports, drugs policy, crime, counter-terrorism and police. OCCRA conduct objective analysis, to help develop, implement, monitor and evaluate government policies and services.

The research team is responsible for providing analytical support to a directorate of the Home Office called the Strategic Centre for Organised Crime, and aims to:

– improve knowledge and fill key evidence gaps regarding serious and organised crime & cybercrime,

– support an evidence-led, policy-making approach; and

– help address objectives set out in the Serious and Organised Crime Strategy[1] and the UK Cyber Security Strategy[2] for tackling and improving UK resilience to serious and organised crime and cyber-attacks.

At a practical level, this involves conducting and commissioning quantitative and qualitative research projects, assessing and synthesising evidence from a range of sources, providing advice and briefing on a wide range of requests from ministers and policy officials, and acting as an interface between policy and academic research in crime and policing.

The OCCRA research programme is principally directed by commitments made in the 2013 Serious and Organised Crime Strategy. The strategy was published to coincide with the launch of the National Crime Agency (NCA), and aims to substantially reduce the level of serious and organised crime affecting the UK and its interests. Based on the framework developed for counter-terrorist work, the strategy has four components:

---

[1] Serious and Organised Crime Strategy (2013), available at: https://www.gov.uk/government/publications/serious-organised-crime-strategy.

[2] The UK Cyber Security Strategy (2011), available at: https://www.gov.uk/government/publications/cyber-security-strategy.

– prosecuting and disrupting people engaged in serious and organised crime (Pursue);

– preventing people from engaging in this activity (Prevent);

– increasing protection against serious and organised crime (Protect); and

– reducing the impact of this criminality where it takes place (Prepare).

Recently published OCCRA work include a report on the criminal careers of organised crime offenders[3], a review of the evidence on cyber-crime[4], an estimate of the scale and costs of serious and organised crime[5], and a report on the nature of online offending[6]. Current analytical projects are focused on: exploring the nature of local markets for illicit goods; the impact of cyber-crime on business reputation; the effectiveness of disruptive tactics aimed at cyber-crime; the extent to which serious organised crime groups are convicted; and economic assessments relating to various new initiatives and policies.

[3] Understanding Criminal Careers in Organised Crime (2013), available at: https://www.gov.uk/government/publications/understanding-criminal-careers-in-organised-crime.

[4] Cyber Crime: A Review of the Evidence (2013), available at: https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence.

[5] Understanding Organised Crime: Estimating the Scale and the Social and Economic Costs (2013), available at: https://www.gov.uk/government/publications/understanding-organised-crime-estimating-the-scale-and-the-social-and-economic-costs.

[6] The Nature of Online Offending (2015), available at: https://www.gov.uk/government/publications/the-nature-of-online-offending.

Crime, Law Enforcement and Sanctions Research Division of the Research and Documentation Centre (WODC), Ministry of Security and Justice, the Netherlands

WODC is the semi-independent research and knowledge centre belonging to and working for the Netherlands Ministry of Security and Justice and its chain partners. WODC conducts social and behavioural scientific as well as legal research. The institute aims to produce knowledge about current and future phenomena relevant to Security and Justice, including policy and programme assessments and forecast (models).

WODC broadly disseminates the knowledge it has acquired. All research results are made available on its own website, while all key and comprehensive research is published in book form or electronically. Moreover, on the basis of its research findings, WODC plays an advisory role with regard to the Ministry of Security and Justice. Finally, WODC acts partly as a granting organisation, since a considerable part of the research portfolio is outsourced to external partners.

The organisation of WODC is made up of the following divisions:

– Crime, Law Enforcement and Sanctions Research Division

– Justice Administration, Legislation, International and Aliens Affairs Research Division

– Commissioning Research Division

– Statistical Data and Policy Analysis Division

– Documentary Information Division

The Crime, Law Enforcement and Sanctions Research Division has about 30–35 staff. It carries out on a broad range of topics. Some major lines of research focuses on organised and economic crime, terrorism, cybercrime, criminal investigation methods, recidivism, and neurobiological factors of criminal behaviour. WODC cooperates with key external research institutes, including the Centre for Information and Research on Organised Crime (CIROC) (a collaboration between WODC and VU University (Amsterdam), Erasmus University Rotterdam, Utrecht University, and Maastricht University) and the Research Network on Organised and Economic Crime.

Dutch Organised Crime Monitor

An important ongoing research project is the Dutch Organised Crime Monitor. The main sources of this research project are files of closed Dutch police investigations of criminal groups. In four data sweeps, during the period 1996–2012, 150 large-scale investigations were analysed systematically. Each case focuses on a criminal network. Together the 150 case reports contain information on many hundreds of suspects. Currently, the fifth data sweep is running, adding 30 new case studies to the dataset. After this fifth round, the Dutch Organised Crime Monitor will include a wide cross-section of 180 cases, covering various crimes, such as different sorts of drug trafficking/production, cybercrime, human smuggling, human trafficking and illegal arms trade, but also (large scale) fraud and money laundering. Each case study always starts with structured interviews with police officers and/or public prosecutors. After these interviews the police files are analysed and summarised. Those files contain the results of all police activities that were deployed in a case, such as wiretapping, observation techniques, undercover policing, gathering intelligence, interrogations, and financial investigation. These sources provide us with a detailed look into the social world of organised crime. Describing and analysing the police files, use is made of an extensive checklist which elaborates upon the following leading questions: What is the composition of the group and how do offenders cooperate? What kinds of illegal activities do they engage in and how do they operate? How do they interact with the opportunities and risks of their environment? What are the proceeds of the criminal activities and how do they spend these proceeds? In addition to the police files, use is made of expert interviews, information from other investigations, confidential reports, crime analyses and (scientific) literature. The case studies of the Dutch Organised Crime Monitor were used to draft four main reports for the Dutch parliament on the nature of organised crime in the Netherlands and numerous scientific articles.[1]

Cybercrime

In recent years, cybercrime has become an important line of research. Besides the EU-funded joint project on organised cybercrime, WODC conducts several research projects on this phenomenon: money laundering in cybercrime

---

[1] Scientific articles have been written on, among other topics: criminal careers of organised crime offenders, investments of organised crime offenders in legal economy, confiscation of the profits of organised crime (first draft submitted), and the role of women in transnational organised crime (e.g. http://english.wodc.nl: Organised Crime Monitor).

cases (running); inventory and classification of cyber security standards (finished); and limits and possibilities of international law for cross-border criminal investigation in cyberspace and the cloud (finished).

Investigation methods and prevention

Another important line of research at WODC is research into methods of criminal investigation and preventative measures. Recent reports include the following topics: undercover policing; wiretapping (including internet tapping); retention of telephone traffic and internet data; human trafficking in the Amsterdam Red Light District: phenomenon, investigation and multi-agency approach; Emergo: a multi-agency approach in Amsterdam; the use of DNA in criminal investigations; prevention of tunnel vision in criminal cases; prevention and identification of sex trafficking; analysis of the national counterterrorism-strategy; and criminal investigation of terrorism.

Recidivism monitor

The WODC Recidivism Monitor is a long-term research project that conducts standardised measurements of recidivism amongst diverse groups of offenders. Measurements are repeated at fixed intervals, in order to follow the subsequent course of the criminal career of the most important groups of offenders.

Neurobiological factors of criminal behaviour

In 2010 the program "Brain & Cognition – social innovation in health, education and safety" started. The purpose of this program is to promote research focused on these areas. The duration of the program is five years: 2010–2015. Within the focus area Safety, which is coordinated by WODC, research is conducted on themes such as: effectiveness of behavioural interventions for severe antisocial behaviour, better decisions under high pressure, resilience or vulnerability to stress, early prevention of antisocial behaviour, and innovative treatments for severe aggression.[2]

---

[2] For further information please visit the website: http://english.wodc.nl/.

The Swedish National Council for Crime Prevention (Brottsförebyggande rådet – Brå) – an agency under the Ministry of Justice – is a centre for research and development within the judicial system. Brå primarily works to reduce crime and improve levels of safety in society by producing data and disseminating knowledge on crime and crime prevention work. The Council produces Sweden's official crime statistics, evaluates reforms, conducts research to develop new knowledge, and provides support to local crime prevention work. The results of Brå's research serve as a knowledge base for the decision and implementation of laws and policies by decision makers within the judicial system, the Parliament and the Government. Brå collaborates on a regular basis with organisations and public sector agencies. The Council also arranges the Stockholm Criminology Symposium, an annual international research conference, on behalf of the Swedish Government. Brå is headed by a director general appointed by the Government.[1]

Division for Research on Economic and Organised Crime (EkoOrg)

The Division of Economic and Organised Crime Research aims at maintaining a national expert function in the field of economic and organised crime. Environmental crime is also part of the Division's research areas. The Division conducts various research projects, often in cooperation with other actors and through external funding, and disseminates this research through various means. The research concerns uncovering the nature of economic and organised crime, primarily in Sweden, with an overarching focus on methods and strategies for crime prevention. Apart from conducting research, the Division regularly takes part in reference groups and responds to referrals. The Division is led by a head of division.

Research strategy

The Division of Economic and Organised Crime Research is largely focused on new and previously unexplored forms of crimes and community action against such crime. During previous years, the Division has published reports

---

[1] For more information please visit the website: http://www.bra.se.

on various topics, such as extortion, corruption and other forms of unlawful influence, money laundering, the financial management of drug dealing, organised tax fraud, social benefit fraud, cultural heritage crime, environmental crime, match fixing, criminal assets recovery, administrative and multi-agency approaches to combat organised crime and money laundering. The research carried out by the Division primarily concerns applied research and development. Based on empirical studies, the Division develops crime prevention strategies and methods together with other agencies within the judicial system. It also cooperates with other government agencies as well as international actors in common research projects. The Division is currently a member of four international research networks through which it takes part in and organises conferences, seminars and publications. There is noticeable interest among government agencies, the public and various organisations for research on economic and organised crime. The employees of the Division give regular lectures on past and current projects, provide expertise advice to government agencies and maintain frequent contact with the media.

Past and current projects

In 2015, the Division published a report investigating how false identities and other types of false official documents are used to commit various types of fraud. The Division also published a report describing the structure of match fixing in Sweden and a report about insurance fraud. The Division of Economic and Organised Crime Research is currently undertaking the following projects:

– Unlawful influence directed at government officials

– Unlawful influence directed at the Migration Agency

– Case study of the multi-agency approach towards organised crime in the municipality of Södertälje

– ARIEL – Assessing the Risk of the Infiltration of Organised Crime in EU MSs Legitimate Economies: a Pilot Project in 5 EU Countries

Unlawful influence directed at government officials

Since 2005, the Swedish National Council for Crime Prevention has studied various forms of unlawful influence – i. e. harassments, threats, vandalism, violence and corruption directed at government officials as witnesses and

plaintiffs. A series of reports on this subject have been published by the Council (e.g. 2005: 8, 2008: 8, 2009: 7, 2012: 12, and 2014: 4) Topics covered in the reports are, for instance: categories of officials at high risk of being exposed to unlawful influence, situations when unlawful influence mainly occurs and examples of parties who exert unlawful influence and the methods they use. Means to prevent and counter proposals have also been presented in the reports. Currently, there are no updated studies regarding the extent of unlawful influence directed at government officials. As a result, the Swedish National Council for Crime Prevention will renew the study/survey made in 2005.

Unlawful influence directed at the Migration Agency

The Migration Agency is the authority performing society's migration and asylum policy, a sometimes controversial topic. Officials within the authority are reasonably exposed to various forms of unlawful influence that may occur in client close relationships. These decisions are often crucial for an individual's future. The study aims to map the influence and pressure that the Migration Agency and its employees are exposed to. Appropriate policies and practices are to be formulated for how this can be prevented and countered. Questions to be answered include: In what kind of context does this happen? What are the consequences? Which kind of unlawful influence has the greatest effect? How can future attempts be countered and prevented? The methods that will be used are interviews, focus groups, participant observation and seminars. The Migration Agency is in need of knowledge about unlawful influence. An in-depth study on this area increases knowledge about the subject of both the authority and the society at large.

Case study of the multi-agency approach towards organised crime in the municipality of Södertälje

In the case study of Södertälje, the multi-agency approach towards organised crime is studied through participatory observations, interviews, and evaluations of investigation files. The project is unique in the sense that it follows the joint agency initiative real-time, thus enabling an in-depth analysis on how cooperation between the different government agencies involved develops. The study is a spin-off from a larger evaluation of the national multi-agency initiative to combat organised crime in Sweden, and is carried out in cooperation between Brå and the Stockholm County Police, Regional CID.

ARIEL – Assessing the Risk of the Infiltration of Organised Crime in EU MSs Legitimate Economies: a Pilot Project in 5 EU Countries

Another project on organised crime is ARIEL – Assessing the Risk of the Infiltration of Organised Crime in EU MSs Legitimate Economies: a Pilot Project in 5 EU Countries. It is an EU-funded project that Brå is finalising together with Transcrime (Italy, coordinators), University of Durham (United Kingdom), Netherlands Institute for the Study of Crime and Law Enforcement (the Netherlands) and University of Maribor, Faculty of Criminal Justice and Security (Slovenia). The project will identify which methods different organised crime groups use to infiltrate, control, and manage legitimate businesses. A special focus is on identifying risk factors, in order to prevent future infiltration. The empirical material consists of intelligence data, investigations, and seminars with experts from public agencies and security staff within the private sector.

Part II

Organised Crime and the Internet:
6th Research Conference on Organised Crime, 2013

The 6th OC Research Conference took place during the 25th to 26th of September 2013 in Niedernhausen, near Wiesbaden. The thematic focus of the conference can be summed up under the heading "Organised Crime and the Internet". Moreover, the conference shed light upon the latest state of research and strategies for combatting especially the existing connection between OC and cybercrime. It provided knowledge on the structure of criminal groups which use the internet and its respective possibilities to communicate in order to commit crimes. Accordingly, relevant "Cyber OC cases" and information on the level of organisation of groups of offenders were shown. Characteristics in preliminary proceedings and legal frameworks were illustrated as well as problems in criminal prosecution and anticipated research demand were discussed. A difference to the previous research conferences was mirrored by the proportional majority of experts from law enforcement authorities presenting their knowledge. This fact could be explained as social science only published contributions within a limited framework regarding the phenomenon of "Cyber OC" in 2013.

Separate articles will not be published about the presentations at the 2013 Research Conference. Because the phenomenon of cybercrime changes so quickly, the presentations from the 2013 conference would no longer be up to date when the book is published in 2016. A summary of the contributions follows:

James Pang, Assistant Director of the Global Complex for Innovation at Interpol Singapore, talked about the activities of Interpol in the field of cybercrime during his presentation about **"Organised crime in the digital age"**.

The Interpol Global Complex for Innovation (IGCI) is a cutting-edge research and development facility for the identification of crimes and criminals, innovative training, operational support and partnerships in Singapore.[1] In the field of cybercrime the IGCI has the task of supporting its 190 member countries with regard to cyberattacks and transnational investigations. This task includes providing a global network with points of contact for cybercrime and database services that are reachable 24/7, as well as identifying emerging threats and informing the member countries about them. Cybercrime is among the fastest growing areas of crime. More and more criminals exploit

---

[1] See http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/About-the-IGCI.

the speed, convenience and anonymity of modern technology in order to commit a wide range of criminal offences. At a global level, the cost of cybercrime is estimated at 110 billion USD. It claims 556 million victims each year, i.e. 18 victims a second. Interpol ocassionally holds working meetings about information technology with a view to enhancing development of strategies and technologies and to providing information about the most recent methods of IT offenders. To illustrate these activities, Pang described several international operations that have been conducted with support from Interpol: In a case of internet banking fraud involving Singapore, a cyber ring used malware bought on the digital black market to access banking data. The fraudulently obtained sums of money were transferred to Tajikistan. The IP addresses of the persons who recruited the money mules were traced to Great Britain. In the "Unlimited Operations" case, during the course of two operations, each of which lasted less than 24 hours, 20,000 financial transactions were carried out in 26 countries scattered across the globe. During the operations, 5 million USD were transferred from the RAKBANK in December 2012 and 40 million USD were transferred from the Bank of Muscat in February 2013. In a case involving pharmaceutical crime, more than 13,700 websites that offered illegal medical products were shut down. A total of 10.1 million harmful pharmaceutical products worth 36 million USD were seized. As part of the SOGA IV operation involving illegal football betting, which was carried out between May and July 2012 during the European championships, almost 300 persons were arrested within the framework of an Interpol-coordinated operation aimed at gambling networks in Asia. Law enforcement agencies in China (including Hong Kong and Macau), Malaysia, Singapore, Indonesia and Vietnam participated in the operation. More than 200 police raids on gambling casinos were conducted. In the context of the SOGA IV operation, a number of international meetings were held with the Interpol National Central Bureaus of the participating countries, including the "Asia Pacific Expert Group on Organized Crime" and training workshops. The last SOGA operation again demonstrated that illegal gambling networks can be combatted by means of police co-operation at national and international level. The various SOGA operations have led to more than 7,000 arrests and the closing of online casinos that had arranged bets worth 85 million USD and have also led to seizure of 27 million USD in cash. The availability of illegal gambling on the internet has increased significantly during the past years. In the meantime banks and credit card companies have been alerted, and they point out suspicious transactions to the law enforcement authorities. The police contact internet providers to make them aware of websites where illegal betting occurs.

"Organised Cybercrime – overview from a Swedish perspective" was the topic of the presentation by **Ulrika Sundling**, Detective Superintendent from the Cybercrime Unit at the National Bureau of Investigation (NBI) in Stock-

holm. In her speech she gave an overview on the responsibilities of her authority and the difficulties of combatting cybercrime.

Sundling gave an overview on the organisation of the National Bureau of Investigation which is part of the National Police Board under the Swedish Ministry of Justice. The NBI's mission can be divided into four parts: Serious organised crime, mobile organised crime and international co-operation and crisis management. The NBI combats serious organised crime, both at a national and international level. The goal is to minimise opportunities for criminal organisations to operate in Sweden. One of the four divisions of the NBI is the Criminal Intelligence & Investigation Division, which acquires, processes and analyses information on serious and organised crime. Operations are focused on narcotics, illegal immigration, human trafficking, money laundering, environmental crimes, child pornography, cybercrimes, homicide investigations and organised crimes. The subordinated IT Crime Unit analyses information and secures evidence during intelligence operations and criminal investigations requiring special IT competence. It disposes on specialists in internet investigations, IT forensics and child pornography. In Sweden, OC has been growing since the year 2000. There are growing statistics related to computer crime and a growing use of the Internet. Drug trafficking, in all its forms, is a crime area traditionally practised by serious organised crime. The smuggling of narcotic drugs to Sweden is dominated by well-organised criminal networks and there are no signs of a decrease in the supply and abuse of drugs. Both trafficking and smuggling of human beings are usually organised by homogeneous criminal networks. Smuggling of cigarettes and alcohol is a very lucrative business and seems to engage increasingly serious criminals. There is a clear development towards more and more serious criminals taking an interest in financial crime, characterised by an interconnection of both legal and illegal activities. Legal participants as well as criminals can be part of criminal plots. One of the most significant threats in the internet is the threat of botnets, which are networks of compromised machines under the control of an attacker. Sundling presented the "Case DDoS" as there were massive DDoS attacks in 2009, the same botnets were used in frauds and also money mules related to OC were detected. The case showed that botnets are used in many different ways, since there was a relation to OC and behind the attacks there was a big criminal network. For online banking services, a banking Trojan is among the most aggressive cyber threats. Almost every banking Trojan implements a "man in the browser" attack, during which attackers are able to inject malicious codes directly into victims' browsers, impersonate them and operate their banking accounts. Regarding the "Case Bank Trojans" it was revealed that it was the work of an extensive organised crime network. In underground forums criminal syndicates are offering "Crime as a Service (CaaS)" that means illegal services, such as infecting large quantities of computers, sending spam and even launching direct denial of service (DDoS) attacks.

The challenges for the Swedish police are conducting complex investigations, often against underground forums, and dealing with the anonymity in computer crime and the encryption of data, which is hampered by anonymization services.

In his talk about **"Onlinebanking-related ID-theft – a case study revealing Cybercrime-related OC"** Erster Kriminalhauptkommissar **Mirko Manske** of Cybercrime Intelligence Operations ("Lage und Analyse Cybercrime") at the Bundeskriminalamt in Germany presented an overview of developments related to cyberfraud in the field of online banking.

Phishing in connection with online banking is probably the best-known type of digital identity theft. In 2013 the Bundeskriminalamt learned details about 4,096 cases of this type. With regard to the opportunities available and the potential profits, phishing continues to be a lucrative field of activity for criminal offenders. For example, in 2013 the average loss suffered when phishing activity involved online banking was about 4,000 euros per case. Following various protective measures such as mobile TANs (mTANs) for online banking and even more intensive efforts to increase user awareness, the number of cases had dropped by almost half in 2012, but in 2013 the numbers were again rising significantly. The main reason is probably that offenders have adapted technically to the changed situation and have developed new or improved malware in order to circumvent security measures. Manske spoke about the number of cases associated with phishing in online banking that were reported from 2005 to 2012 and pointed out the constantly increasing numbers, but also the temporary decline in these numbers following introduction of security measures such as the i-TAN system. He contrasted these numbers with BKA estimates of actual case numbers, because many cases are not reported. He presented different cases to illustrate the modi operandi of online fraudsters. In a 2006 "dinosaur phish" case, a spam message was used to lure customers to a fake banking page where, allegedly due to new security measures, customers were asked to click on a link and provide TAN numbers and access data. After i-TANs were introduced starting in 2008, the "man-in-the-middle" attack established itself as an attack vector. The customer received an e-mail with malicious software (malware) in the attachment. When the attachment was opened, a Trojan horse was installed on the customer's computer. The customer then logged into the online banking system with his password. The Trojan horse was used to change the recipient and the amount of money transferred. After this, the bank required an i-TAN number to confirm the transfer. The customer thus authorised the fraudulent money transfer. When such a "man-in-the-middle" attack occurs, the attacker is located either physically or logically between the two communicating parties and controls the data flow between these parties by means of his system. During the attack he can see the information in question and manipulate it. The increasing po-

pularity of mobile terminals such as smartphones and the lack of user sensitivity to the digital dangers posed by these devices meant that such offences remained attractive for the perpetrators. Among other things, this was demonstrated by an increase in malware programmed for the operating systems of mobile devices. From 2006 to 2010, money mules were often recruited for phishing associated with online banking that involved fraudulent transactions. Phishing "shops" were used for recruitment. From approximately 2010 to 2012, criminal infrastructure services were the dominant business model: Several infrastructure providers cooperate or compete simultaneously in the global marketplace, offering specialised services such as provision of money mules. In 2012 the ZitMO (Zeus-In-The-Mobile) vector attack emerged. When this modus operandi was used, the malware on the respective device, which had been infected by a Trojan horse, manipulated communication in the web browser so that the information relayed was different than that provided by the user. The victim's smartphone was infected with malware by using a Trojan horse sent via a text message. As soon as the victim logged into the respective banking portal with his access data, the fraudsters used the ZeuS Trojan to intervene in the banking transaction and prompted the victim to enter the type of smartphone and the phone number in a popup window. When the victim did this, the device was infected. The Trojan was employed to transmit the data to a Command and Control server. The perpetrator's server generated a text message instructing the user to update the smartphone. A WAP link to an infected website was in the text message. Another modus operandi is selling already infected smartphones, for example through eBay. Beginning in 2013, so-called "runners" emerged, whose task was to withdraw the respective sums of money from cash dispensers and who were traded and exchanged by the criminal groups to perform special services for them.

Edwin Kruisbergen, researcher at the Research and Documentation Centre of the Dutch Ministry of Security and Justice, gave a presentation titled **"Digitized organised crime: traditional organised crime and ICT"**.

Traditional organised crime includes drug trafficking, human smuggling, human trafficking, illegal arms trade, and money laundering, among other criminal activities. Edwin Kruisbergen focused on drug trafficking. In the first part of his presentation he discussed how ICT (Information and Communications Technologies) may be used with regard to the different activities and assets that are necessary for a drug trafficking operation: logistics; communication; social capital; and money laundering. Concerning the logistics, for example, Kruisbergen used recent criminal cases to illustrate how offenders use ICT to facilitate the production, distribution (sell), and smuggling of drugs. With regard to the *production* of drugs, the internet is used to purchase precursors, such as GBL (Gamma-Butyrolactone) which is used to produce GHB (Gamma-Hydroxybutyric acid = liquid ecstasy). Dutch individuals imported

thousands of litres of GBL from China and sold it on the internet. „Dutch" GBL has been found in many countries; from Germany to China. In other cases offenders engaged in the production of synthetic drugs used the internet to purchase pill making machines. Furthermore, several black markets on the deep web are used to *sell* drugs. Examples of these black markets are Silk Road, Black Market Reloaded, and Atlantis. Another important step in drugs trafficking is *transportation and smuggling*. A few months before the research conference, nine people were arrested in an unique case of 'digitized' drug smuggling. Hundreds of kilos of cocaine were seized, as well as hundreds of kilos of heroin, and more than a million Euros in cash. The offenders used ICT to facilitate the smuggling of the drugs through the port of Antwerp; they hacked the computer network of container terminals and shipping companies. As a result the offenders could manipulate the time and place of unloading of containers in which co-offenders hid drugs.

Thorough empirical research on the use of ICT in traditional organised crime is scarce. In the second part of his presentation, therefore, Kruisbergen explored the main questions that should be on the research agenda concerning ICT and organised crime. A very basic question relates to how serious – how widespread and advanced – the use of ICT actually is. But there are many other questions. How do offenders who participate in organised crime activities use ICT? What consequences does the use of ICT have on other aspects of an organised crime group? Does the use of modern communication technology alter the way in which criminal groups are organised? Does ICT help offenders to solve specific bottlenecks in their modus operandi? Does the use of ICT perhaps introduce new bottlenecks? Does the use of ICT have consequences for the markets and levels on which a group operates? With regard to normal, legal enterprises, it is often said that the internet is *a* or perhaps *the* most important stimulus behind globalization. Does that also hold for criminal enterprises? Other questions relate to the offenders themselves. Are the 'usual suspects' using new technology, or does the new technology come with a new kind of offenders?

If empirical questions such as these, and others, are answered, more theoretical questions may be addressed. Ultimately, according to Kruisbergen, the most important question is: if traditional organised crime becomes (partially) digitized, should this have consequences for our understanding of OC? In other words: are theoretical insights and concepts that were developed in reference to offline operating criminal groups, such as the social embeddedness of organised crime, still valid when we look into the modus operandi of digitized organised crime? One such concept is the *social embeddedness* of organised crime. One of the most important assets for offenders in organised crime is social capital. In order to participate and succeed in organised crime activities, one has to know the right people; buyers, sellers, producers, trans-

porters, co-financers, money launderers and so on. Since most criminals do not advertise, they have to rely on social relations, i. e. they have to find capable and reliable offenders in their social network. One could ask whether 'knowing the right people' will transform into 'knowing your way on the deep web'. Will the internet diminish the importance of real life social capital? Answering questions such as the above is quite an ambitious task. However, Kruisbergen argued it is necessary to address them if we really want to understand how ICT is changing organised crime.

Dr. Melvin Soudijn, Senior Researcher in the High Tech Crime Team of the Dutch National Police Services Agency in Zoetermeer, spoke in his presentation **"Offender Convergence Settings in Cyberspace"** about the results of an analysis directed at an internet forum.

The designation "Offender Convergence Settings" (OCS) was first used by Felson[2] in 2003 to describe physical locations in which (potential) offenders meet with each other. This is where they meet with friends, make new acquaintances, exchange information, sell stolen material or plan new criminal acts. Offender convergence settings provide structure and continuity for the individual and the network. In his project, Soudijn analysed whether offender convergence settings also exist in cyberspace. Previous analyses have shown that cybercriminals meet in virtual space, including in carding forums. Carding refers to the wrongful use of personal data from bank and credit cards (Peretti, 2008). Some of the forums are open to anyone interested in this form of criminal activity, while others are extremely difficult to access.

Investigations by the National Police uncovered one of these carding forums in 2008. Even though the forum was blocked for persons unauthorised to access it, a technical defect made it possible to create a digital copy of the contents. This provided the police with extraordinary insight into the unlawful activities of the cybercriminals. Soudijn carried out a textual analysis of almost 154,000 postings by more than 1,800 members of the carding forum from 2003 to 2008. The data were compiled in connection with a "Social Network Analysis" (SNA). The real identities of the members were not determined; only their nicknames were learned. The carding forum had two functions: providing a place to exchange information (knowledge place function) and a place where offers of and searches for products and services were possible (market place funtion). On average, each forum member was in contact with 16 other persons. New members established a number of contacts within a very short period of time. The various criminal groups also came into contact with each other. Some of them trafficked in stolen credit cards or mal-

---

2   Marcus Felson, Texas State University (2003).

ware, others carried out money transfers, and others handled the graphic design for creating false websites or acted as intermediaries for finding anonymous servers. Arrangements for the commission of criminal offences were not made in the forum. The forum administrators tried to recruit trustworthy members. They created a system with guarantees, peer review and status. Membership in the forum required a payment of 50 USD. After the money was paid, a user name and a password were issued. Access to the forum required naming two forum members as references. A peer review system was used to evaluate the goods and services offered as well as the trustworthiness of the person concerned. As in eBay, an individual with numerous positive evaluations is considered to be more trustworthy than other persons with no feedback. In addition, forum members were assigned a status as Moderator, Newcomer, Service, Member, Verified Member, Administrator, Deer (violated forum rules), Unresolved Problems or Ripper (cheated other forum members). Textual analysis was used to identify the four phases of carding: 1) preparation 2) commission of the theft during which the bank or credit cards are stolen 3) the "money mule" phase during which the money is transferred by a money mule 4) The "cashing phase" when the fraudulently obtained money is obtained by the main suspect. Analysis of the communications in the carding forum also revealed that hacking bank accounts or obtaining money by fraudulent means is not the main challenge faced by cybercriminals. Rather, the challenge is how to avoid leaving behind traces when the money is transferred to other accounts. Soudijn explained that it is difficult for law enforcement to gain access to criminal forums. They are located on servers for which there are no geographical borders. However, at least the Dutch project did gain some insights into this phenomenon.[3]

In her speech **"In the meantime in cyber space …" Floor Jansen**, Advisor of the Team High Tech Crime at the Dutch National Police Services Agency in Driebergen, talked about an international child pornography case and the difficulties for law enforcement agencies to reveal anonymous sites in the internet.

Jansen described that in the end of 2010 a photo of a two year old boy with a plush toy was detected in the Internet. The victim was identified by the Dutch Police. A man from Amsterdam who possessed pornographic files from 84 children was investigated as producer of the pornographic site. He mainly used the social network ICQ establishing contacts to children in 53 countries. 440 chatlogs could be secured, assigned to 1,116 nicknames. In the frame-

---

[3] Quite a bit of additional information is available in the publication "Cybercrime and virtual offender convergence settings", Authors: Melvin Soudijn and Birgit C.H.T. Zegers, published on 25.05.2012 in „Trends in Organized Crime". http://link.springer.com/article/10.1007%2Fs12117-012-9159-z#page-1.

work of the investigations 80 further cases became known. The Internet Relay Chat (IRC), a text-based chatlog which allows roundtables in channels and between two participants (query) was also used. Producers of pornographic material are mainly difficult to identify because they usually only have access to porn sites to set new material. The investigations led to the TOR anonymity network, also described as "The Onion Router", a system that allows users to mask their location and communicate anonymously. TOR is part of the deepnet which does not get indexed by search engines like Google. By the website monitoring tool DSRT, a network crawler was developed to find further relevant websites. The Dutch agents systematically visited each of the identified sites and made a list of those dedicated to child pornography. Many other criminals were acting in TOR. On the whole, 450 relevant sites with a collection with 220,000 photographs and videos were found, 33% of the material was new. Ten of the illegal sites were destroyed and spammed with the Dutch Police logo and the text "This site is under criminal investigation by the Dutch National Police. You are not anonymous. We know who you are. The production, distribution and possession of child pornography are serious crimes. All information gathered in this criminal investigation will be shared with the appropriate authorities." One of the illegal websites only lasted for two weeks. The Dutch Police worked together with the FBI, which in 2012 started the "Operation Torpedo" in the United States. With a search warrant from the Court of Rotterdam, the U.S. agents set out to determine where the sites were located.

The pornographic case is an example of a classic detective case with a digital twist. The whole operation showed how international authorities can work together and it could be a warning for criminals that the internet is not as anonymous as everybody presumes it to be.

In his presentation on **"Cybercrime and Threat Convergence" John T. Picarelli, Ph.D.**, Program Manager for Transnational Issues at the National Institute of Justice (NIJ), U.S. Department of Justice, provided an overview of the threat posed by cybercrime in the United States, discussed links to organised crime and terrorism, and described the approach taken by the United States to combating this phenomenon.

The NIJ is the research, development and evaluation agency of the U.S. Department of Justice. The Institute conducts research on crime phenomena and legal issues and deals with the fields of social science, forensic science and technology. The "Transnational Issues" department maintains contacts throughout the world. The NIJ conducts research on "threat convergence", the interaction between two or more threat scenarios and their influence on illegal markets. Of particular interest here is how these threat scenarios affect illegal markets on the internet. Michigan State University has analysed the development of new illegal markets on the internet. In this connection 13 web

forums, ten in the Russian and three in the English language, were studied, forums that serve as places to pass on stolen account information, etc. It was determined that 84% of the data offered there were stolen; 45% of the data were credit card or account data, with most of the data coming from Europe. A clear division of tasks in the online networks was established. The sellers are the central figures. The networks lack transparency, and a hierarchy seems to be lacking. In the United States, increasing numbers of websites for prostitution and human trafficking are being created, a development promoted by social media such as Twitter, Facebook and YouTube. The organisation "Shared Hope International" identified more than 5,000 persons associated with trafficking in women. In seven American states it was established that the sex trade has been growing steadily on the internet since the 1990s. This applies in particular to the distribution of illegal videos.

Terrorist organisations use the internet to recruit violent extremists and prepare attacks. However, thus far little information is available in the United States about self-recruitment and self-radicalisation via the internet. Brandeis University, in the American state of Massachusetts, has collected important information about the role played by the internet in connection with the recruitment and radicalisation of violence-prone extremists in the United States who support Al-Qaeda, Hezbollah and Hamas. The average age of extremists who support Al-Qaeda is over ten years less than the average age of those who support Hezbollah or Hamas. The current trend is that the supporters are becoming even younger. With regard to the effect of using social media, it was established that the time from initial radicalisation to commission of a criminal offence or arrest decreased from 6 years prior to 9/11 to 1.7 years after 2007. Studies about DIY (do-it-yourself) terrorism have shown that radicalised individuals find rules of conduct in internet networks. In 2013 a project about the factors that influence radicalisation associated with transnational organised crime began. Interviews with 100 supporters imprisoned in the United States are planned. Information is to be collected about the expertise that members of international OC networks need and to what extent they involve legal institutions in their criminal activities. Good connections with the private sector in the form of public-private partnerships are considered to be very important for fighting cybercrime. This is because the private sector controls the infrastructure of the internet. Picarelli pointed out the good co-operation to be found in the European CIRCAMP project (Cospol Internet Related Child Abusive Material Project) in the field of child pornography. 14 European countries, supported by Europol and Interpol, are project members. CIRCAMP is supported by the "EC Safer Internet Programme" of the European Commission, and it cooperates with affected countries throughout the world. In closing, Picarelli emphasised that international co-operation between American and European authorities is desirable and necessary.

In his presentation entitled **"Transborder investigations in cybercrime cases – New challenges for law enforcement" Rainer Franosch**, Public Prosecutor in Charge at the Central Department for Combating Cybercrime of the General Public Prosecutor's office in Frankfurt am Main, described the challenges presented by cross-border investigations into cybercrime.

In his presentation, Franosch pointed out the increasing professionalism of cybercriminals, who use new technologies to commit offences. He spoke in greater detail about the possibilities available to law enforcement agencies in Germany that deal with cybercrime. The office of the General Public Prosecutor is responsible for investigative proceedings in cases of terrorism, espionage, treason and genocide. Since June 2011, the Central Department for Combating Cybercrime (Zentralstelle zur Bekämpfung der Internetkriminalität – CDCC) has been the public prosecutor's office responsible for urgent cybercrime cases throughout Germany. The cases that it handles are often internationally oriented and are frequently handled in co-operation with the U.S. Secret Service and the FBI. In the meantime several of the German states now have units in their law enforcement agencies and public prosecution offices that specialise in cybercrime. The general public prosecutor's office of any German state can conduct cross-state and trans-national investigations. Obtaining electronic evidence across borders is a great challenge for the law enforcement agencies. The agencies are confronted with the problem of securing evidence in cases where the place of the offence has not been established ("loss of location"). Franosch referred to the continuing discussions about possible legal solutions to the problems presented by the "loss of location" of data stored on the internet. In the case of cloud computing, to an increasing extent software associated with large amounts of data is moving to the internet. In the process, the clouds are constantly being shifted from one server to the next and are moving through various countries at indeterminable times. They can also be at different places within a country or in different countries. Even the providers of cloud computing services are probably often unable to determine where data are located at a specific time. This means that the data are located in different jurisdictions/legal systems, which creates significant problems for law enforcement. Computer data are often stored outside the respective national territory. Conducting a transborder search for these data must be regarded as a violation of the principle of territoriality. Thus, strictly speaking law enforcement agencies are not permitted to conduct any searches in the internet as soon as the possibility of exceeding the limits of their own national territory exists. With regard to cross-border law enforcement, cases where the data relevant to an investigation are stored on servers in other countries are becoming increasingly common. In such criminal cases, traditional channels of international co-operation are often too slow, which leads to loss of evidence. Requests for mutual legal assistance, a traditional instrument of transnational co-operation, are usually ineffective

when investigations involve the internet. When investigations are conducted in the internet, the time factor plays a decisive role due to the lack of data retention in some countries. Law enforcement agencies are nevertheless obligated to pursue crime in the internet. In the 2001 "Budapest Convention on Cybercrime"[4], transborder access to data is regulated. According to Franosch, the Convention does not provide adequate opportunities for investigations in urgent cases. In particular, it is unsatisfactory in cases where rapid access is needed to data stored abroad that is not freely available. Implementation of an international agreement for gaining access to data stored on servers in third countries is of decisive importance. Franosch claims new operational partnerships are needed at international level, not only for the police but also for public prosecutors' offices, in order to combat cybercrime and money laundering on the internet.

In his brief presentation entitled **"Cybercrime Networking: Important to criminals, essential for policing"** Supervisor Special Agent **Brian T. Herrick**, Federal Bureau of Investigation, informed his audience about the jurisdiction of the FBI in the field of cybercrime and his work as a liaison officer for the United States in Germany.

The FBI is a security agency with responsibilities in the field of law enforcement and also in the field of intelligence. Among other things, it is responsible for combating cybercriminals and highly technological attacks. The FBI has more than 60 offices abroad called "legal attachés", which are located in U.S. embassies worldwide. Partnerships with international law enforcement agencies are necessary in order to combat effectively the threat posed by cybercrime. The modern investigator in the field of cybercrime needs to understand the laws and investigative possibilities of both his own country and other countries and must also be able to implement them. To do this effectively, personal contacts and partnerships have to be established. In the field of cybercrime, the FBI works closely with industry and international partners. To ward off cyberthreats, the "National Cyber Investigative Joint Task Force" (NCIJTF), in which 19 agencies from the fields of law enforcement and intelligence cooperate, is located at the FBI. In Germany, links to the United States are frequently established on the basis of an IP address and/or an ISP that has been identified. Law enforcement agencies in the United States are very active in the battle against cybercrime and are among Germany's most important co-operation partners.[5]

---

[4] German text of the Convention "Übereinkommen über Computerkriminalität", Budapest, 23.XI.2001 (Revised translation agreed upon by Germany, Austria and Switzerland): http://conventions.coe.int/Treaty/GER/Treaties/Html/185.htm.

[5] For further information, see: http://www.fbi.gov/about-us, http://www.fbi.gov/about-us/partnerships_and_outreach/.

Part III

The different Faces of Organised Crime:
7th Research Conference on Organised Crime, 2014

The 7th OC Research Conference on Organised Crime was conducted at the Bundeskriminalamt in Wiesbaden during the 8th and 9th of October 2014 and focused on "The Different Faces of Organised Crime". The thematic focus of the OC Research Conference 2014 lay on the research efforts and the illustration of the situation with regard to the faces of OC. Six out of the eight speakers referred to OC in Germany, the UK, the Netherlands and Sweden. One of the presentations from Sweden reported a new form of criminality of OC, namely benefit fraud. Benefit fraud is classified as belonging to OC provided that it is committed in an organised way. Moreover, Sweden presented the "Arboristic Approach" for combatting OC. This was further elaborated on as a representative of the National Crime Agency (NCA) in London pictured the British strategy for curtailing OC in 2014/2015. The Netherlands provided reports on the production of synthetic drugs from chemical precursors and revealed the implementations of the insights from the analysis of OC proceedings on the approach of criminal prosecution in order to combat OC. The German presentation mirrored the respective forms of OC occurring in Germany. Other presentations included faces of the Russian Mafia in Eurasia and Europe and reported upon the functions and goals of the "Global Initiative against Transnational Crime".

The Deputy Head of the Division "Serious and Organised Crime" at the Bundeskriminalamt Germany, Leitender Kriminaldirektor **Stefan Michel**, described various aspects of serious and organised crime and provided an overview of the most recent developments and challenges for the police in his presentation entitled "**The different faces of organised crime**".

For the past ten years, the number of organised crime proceedings conducted in Germany has been around 600 per year. The German organised crime report, which covers about 600 organised crime investigations and 9,000 suspects anually, does not provide a comprehensive picture of the situation created by this form of extremely serious crime. Collection of information about these investigative proceedings is based on a narrowly formulated definition of organised crime that only includes especially serious modi operandi. The approximately 600 organised crime investigations each year are associated with 1,500 to 2,000 investigations of offences possibly linked to organised crime and, in addition to 9,000 organised crime suspects, approximately 20,000 to 30,000 serious and very serious offenders are also the subject of suspicion. Michel provided an overview of cybercrime, traditional and new forms of organised crime groups, and the forms of crime that characterise the "face" of organised crime in Germany, which are described in the following.

In Germany, there are approximately 9,000 members of **outlaw motorcycle gangs** organised in about 650 chapters. The phenomenon of outlaw motorcycle gang crime is of considerable significance and requires a great deal of attention from the law enforcement authorities, especially because this phenomenon has become more multifaceted, complex and difficult to assess. Outlaw motorcycle gangs have been attracting an increasing number of new members and supporters. The focus of attention is not limited to traditional established outlaw motorcycle gangs. The numerous support clubs, groups similar to outlaw motorcycle gangs, and street gangs founded recently represent an additional potential for conflict with regard to disputes among themselves and with the established groups. Outlaw motorcycle gangs are networked at an international level and sometimes cooperate with other organised crime groups.

In Germany, **Russian-Eurasian organised crime structures** have established themselves firmly over the years. Russian-Eurasian organised crime views itself as a parallel society with its own system of norms and values. The ideology of the "thieves-in-law" is rooted in segments of the Russian-speaking community in Germany – a group of about 4.5 million people. This ideology is particularly widespread in German prisons, where approximately 4,500 to 5,500 Russian-speaking or ethnic Russian inmates are serving sentences at any one time. European investigating authorities focus in particular on Russian-Eurasian groups of criminals that come to attention in connection with organised crime, generally property crime in the form of shoplifting or burglary.

For the **Italian mafia**, Germany continues to be above all a safe haven and place of retreat. A total of 244 organised crime proceedings were conducted against Italian OC groups during the past 15 years. In the mid-1990s a German-Italian working group prepared an overview of mafia members located in Germany. Among other things, from 1995 until the present, their work led to the arrest of 314 mafia members in Germany for committing various criminal offences in Italy, including several murders. In addition, since the murder of six persons in the German city of Duisburg in 2007, there has been a German-Italian task force that works to optimise the exchange of police information and intensify operational cooperation.

There are also forms of criminal activity that, as presumed mass crime, must be considered at least as gang and commercial crime, while in some cases such crime is also embedded in OC structures at international level. **Organised fraud committed through call centers** is among these forms of crime. For several years now, there have been offences of fraud initiated by call centers that are located primarily in Turkey. The callers promise winnings in return for advance payments, or threat scenarios are created and unjustified de-

mands are made. Most of the victims are older people, and the percentage of the crimes reported is estimated to be 10% at the most. The perpetrators act in an organised manner, operate across borders, and divide up their tasks. Their communications using VoIP are generally manipulated to conceal Turkey as the source of the calls and to hinder police investigations.

Another example is **structural property crime involving the burglary of dwellings** that is committed by traveling groups of perpetrators. Until 2006, the number of cases involving the burglary of dwellings declined in Germany. Since then, the number of cases has increased steadily. The increase is due primarily to perpetrators and groups of perpetrators from Southeastern and Eastern Europe. The perpetrators travel to Germany from other countries for the purpose of committing criminal offences. Some of them stay in Germany for weeks, or even months, in order to break into dwellings or commit other offences. They often use the services of so-called "residents", usually fellow countrymen, who arrange to obtain vehicles, dwellings and papers and who also arrange for attorneys if any arrests occur. In addition, the "residents" provide information about appropriate buildings and areas to burgle and handle the disposal of the stolen property.

The presentation on **"Mafia and Anti-Mafia in Eurasia: the Specificity of Post-Soviet Georgia"** by **Dr. Gavin Slade**, Criminologist and Research Fellow at the Free University Berlin and Dahlem Research School aimed at examining the role and impact of Georgia in organised crime. His findings are based on research done during the last seven years.

He claims that a vast number of Russian Mafia members were arrested due to various incidents like Operation Java in 2010 or the "Yaponchik" assassination in 2009. Furthermore, it was concluded that it is quite puzzling that Georgians make only two percent of the Soviet population but one third of initiated thieves-in-law are Georgians. With regard to the background, it was explained that thieves-in-law are a Gulag legacy and emerged at the end of the 1920s. Slade went on to explain the aforementioned juxtaposition: The reason why Georgians are to such an extent involved in OC is related to the end of the Soviet Union which provoked a big state collapse in Georgia. Of all the ex-Soviet republics only the state collapse in Tajikistan was bigger. Therefore, there was a serious demand for security and protection services in Georgia. Moreover, Georgia had one of the biggest black markets in the Soviet Union and the romanticizing of thieves in Georgian society which takes also place in the socialization of children is mirrored in a survey from 1993 in which it was assessed that 25% of Tbilisi school children wanted to be a thief-in-law. However, this situation has undergone drastic changes, according to Slade, due to the Rose Revolution in 2003 and a very rigorous anti-mafia legislation as well as huge reforms that were borrowed from Sicilian cam-

paigns and models. This could also be seen in the number of prisoners which tremendously increased from 6,119 in 2003 to 23,864 in 2010. Moreover, the 'zero tolerance' politics of Georgia can be seen in the citation from Micheil Saakaschwili, former president of Georgia from 2004–2013: 'Our biggest export to Russia is no longer wine but thieves-in-law.' and accordingly, 10 percent of Georgian thieves-in-law went to Europe, Israel and CIS. It is also noteworthy that most thieves derive from only three Georgian regions, amongst others Abkhazia. Members of the post-Soviet OC are very well interconnected and dispose on a high mobility. This seems to be a Gulag legacy, however, the transplantation of the crime groups in foreign countries is difficult. It was explained that the thieves-in-law emerged from a relatively homogenous penal subculture. The subculture developed practices, e.g. the code of honor and tattooing, to deal with uncertainty due to camp structure and the high turnover and movement of prisoners. Enclosing, it can be stated that mobility led to the strength of the thieves-in-law. As a result, Slade summarized that the old mechanisms that enable collective action and coordination enable the spread of post-Soviet OC besides the fact that the thieves also work across ethnicities.

The presentation entitled **"The Global Initiative against Transnational Organized Crime- Exploring new Challenges and Responses"** which was held by **Ambassador Dr. Ugljesa Zvekic** concerned the establishment of The Global Initiative against Transnational Organized Crime and examines its history, challenges, goals and context.

In the following paper, it was stated why "The Global Initiative against Transnational Organized Crime" came into life. Firstly, it was elaborated on the impact and extent of OC which has changed its scale and scope dramatically over the past years. Not only have shifts in major illicit markets occurred, but in particular with reference to fragile states, OC poses an enormous threat as it accumulates criminal activity as well as it spreads insecurity and violence when exercising control over groups of people. Even in relation to more developed states, OC has a vast impact on stability, governance and development. Moreover, there are only few international conventions in the area of OC; the most important one is the Palermo Convention. However, there are claims the Palermo Convention is biased towards law enforcement authorities; it is outdated, not effective and too old. Therefore, a new platform for strategic engagement was required and the foundation of the Global Initiative resulted from the aforementioned fact, although it is not a convention but a network of different actors which derives from off the record discussions. The objectives include strategic, analytical and responsive approaches in order to evoke more effective responses to OC, e.g. to enhance the awareness and stimulate the discussion over nature, extent and solutions to the OC problem besides creating a network with resources for international partnerships. Next,

the structure of the initiative was explained which consists of more than 100 participants, an advisory board and a secretariat based in Geneva for which the Swiss government provides premises. Notably, the initiative is not led by the government and it has a distinct approach which provides it with more flexibility as it does not have to take political considerations and arguments into account. Prioritized areas within the framework of the initiative include environmental crime, governance, state and development fragility and cyber-crime. Furthermore, Zvekic called attention to various priorities including programs and dialogues on specific topics in order to raise awareness and make progress in the respective areas. In closing, he pointed out that the initiative has not reached all goals yet as there is still a tremendous amount of problems to tackle. Until now an evaluation of the implementation of the Palermo Convention in the different countries is missing, for the evaluation is blocked by several governments. Furthermore it was stressed that we also have to bear in mind that OC is directly connected to poverty, education, access to micro-credits etc., thus an holistic approach is necessary and not only the view of governments and law enforcement authorities, as we have to tackle and analyse OC in combination with development questions. Nevertheless, this combination does not seem to be realizable because theories of OC and theories of development are still separate. Lastly, Zvekic assessed that the Global Initiative also includes questions like: 'Does the legalisation of drugs/marihuana have consequences for OC?' and therefore addresses burning political questions and brings them to discussion.

Scientific research and police practice was the subject of the presentation by **Prof. Dr Edward Kleemans** from the VU University in Amsterdam, Faculty of Law. In his lecture titled **"Organised crime as transit crime and what it means for criminal investigation",** Kleemans talked inter alia about the structure of organised crime in the Netherlands, the Dutch "Organised Crime Monitor" and how the insight into organised crime structures led to a change in criminal investigation strategies, international cooperation and prevention.

Kleemans described that the structure of OC groups in the NL is mostly not a pyramid, like in Italian mafia groups, but rather a network of criminals. OC groups do not make the most profit locally, but rather with smuggling and trafficking. So their offences have an international context. Transit crime is therefore dominant in the Netherlands. Transit crime focuses on trade and on crossing borders. He emphasized that studies of transit crime show that many regular businesses are involved in the logistics of transit crime, such as transport companies, expedition companies, travel agents, etc. Profitability is the major reason why "transit crime" seems to be the main activity of many organised crime groups. This is true for drug production as well as import and export. Handsome profits can also be made by smuggling illegal immigrants

and highly taxed goods. To get a better insight into the nature of organised crime and to improve policies and police practices, the Dutch Research and Documentation Centre got the mission to conduct the continuing research project "Dutch Organised Crime Monitor". In the framework of this Monitor a report based on an analysis of 40 major police investigations into criminal groups in the Netherlands is published every four years. Information is also drawn from publicly available and confidential reports, from crime analysis reports and from interviews with experts in the field. During the period 1996–2012, 150 large scale investigations were systematically analysed.

The systematic empirical research (Dutch Monitor) led to three consequences:

1. consequences on investigation strategies

Nowadays the Dutch law enforcement authorities focus on important persons in a group (facilitators) and no longer only bosses/leaders of the group as main objective. Facilitators are often more important than the boss as they keep the group operative.

2. consequences on international cooperation

There is now more international cooperation with a permanent exchange of knowledge and information, taking into account the priorities of the partner countries and the transfer of responsibilities from local to national level.

3. consequences on prevention

Research showed that there are certain opportunities for crimes. Therefore, the 'barrier model' was developed. The barrier model looks at trafficking as a business enterprise that has to overcome a series of barriers before the traffickers can start making money from the exploitation of others. The aim is to increase the "height" of the barrier traffickers face, so that trafficking in human beings becomes more difficult, less lucrative and thus less attractive. The barriers are: recruitment, entry, identity, psychological attachment, housing, work and financial aspects.

Another major change during the last decade was the increasing usage of flexible, prompt intervention strategies as an alternative to the large-scale and lengthy police investigations of the past. Arrests and seizures in criminal networks were no longer postponed or prevented at any cost, but were – on the contrary – sometimes used deliberately to gather evidence against the prime suspects. Prompt interventions are now often combined with a more long-term investigation strategy. It was also accompanied by a stronger focus on facilitations in criminal networks and the role of the facilitating environment.

The so-called administrative approach, involving local governments and other partners in fighting and preventing OC, is now a widely acclaimed and accepted approach towards OC in the Netherlands.[1]

In his presentation entitled **Trends and developments in Dutch synthetic drugs crime**, **Matthijs Vijlbief** from the Central Intelligence Division of the National Police of the Netherlands described the manufacture of synthetic drugs in the Netherlands, especially amphetamines.

According to Vijlbief, the Netherlands is probably the main country of production for synthetic drugs worldwide. In 2013, 57 drug laboratories and 120 storage facilities for amphetamines and MDMA (3,4-methylenedioxy-N-methylamphetamine) were seized. Estimated annual production amounted to 80,000 kilograms for amphetamines and 150 million tablets for MDMA. The annual turnover of such illicit wholesale trade amounts to 200 million euros. This means that the street value is two billion euros. PMK (piperonyl methyl ketone), BMK (benzyl methyl ketone), GBL (gamma-butyrolactone), ephedrine and lysergic acid are important chemicals for manufacturing synthetic drugs. In Asia, PMK is extracted from safrole-rich oils found in tree roots. There is very limited legal use of PMK for the manufacture of perfume. Its manufacture has been subject to international controls since the the Vienna Convention of 1988. It is transported from China to Western Europe, especially the Netherlands, and used for the illegal manufacture of MDMA. One litre of PMK yields one kilogram of MDMA, which can be used to produce 10,000 ecstasy tablets.

BMK, which came from China in the past, is produced both legally and illegally in chemical factories in the Netherlands and used for the production of amphetamines. The substance is used legally to produce rat poison, for example. Production has been subject to international controls since adoption of the 1988 Vienna Convention. Pre-precursors are chemicals used to produce precursors for the manufacture of illegal drugs. Their manufacture usually requires only one addtional, often even legal, process. A number of pre-precursors are produced in the Netherlands. For example, in 2010 a police search resulted in seizure of two tons of the substance APAAN (alpha-phenylacetoacetonitrile). It is a grey-white powder that is an exteme health hazard for the skin, eyes and respiratory system. Due to suitability as a pre-precursor for

---

[1] More information on: "Applied Police Research – Challenges and Opportunities", edited by Ella Cockbain and Johannes Knutsson, Crime Science Series, Book Routledge, first published 2015; Contribution of E. R. Kleemans: "Police data and academic research", https://books.google.de/books?id=kaDBAAAQBAJ&pg=PA64&dq=Kleemans+investigation+strategies&hl=en&sa=X&ved=0CCAQ6AEwAGoVChMIlrXrwtfhxgIVwrgUCh0ZkwTy#v=onepage&q=Kleemans%20investigation%20strategies&f=false.

methamphetamine synthesis, phenylacetones are prohibited in the European Union and in Switzerland. The first seizure of a laboratory for converting APAAN to BMK took place in February 2011. There is no legal use for APAAN. Since the end of 2011, the Netherlands has been flooded with APAAN produced in China. Until the end of 2013, there were no restrictions on producing and trading this substance in the entire European Union. It is assumed in the Netherlands that, in 2012, 50% of all seized amphetamines (speed) were produced using APAAN, while in 2013 the percentage had already risen to 75%. The increasing significance of the substance is due to the fact that the precursor BMK can be obtained by using a simple chemical process. Three different conversion methods can be used for this purpose: 1. with sulphuric acid, which makes it possible to utilise about 60% of the substance; 2. with phosphoric acid, which already increases utilisation to 70%; 3. with hydrochloric acid, which results in 80% utilisation for production of BMK. The highest quality is obtained by using sulphuric acid. It is most effective to use hydrochloric acid, but this represents the greatest danger to health. Using APAAN results in larger profits for the drug producer: In the past, it cost 800 euros to produce one litre of BMK, but now it only costs 60 euros. However, the wholesale price for one kilogram of amphetamine has remained the same. This has resulted in the increased availability of BMK. The number of production facilities rose from 36 in 2011 to 66 by the end of 2014, and the number of storage facilities increased from 61 in January 2011 to 228 by the end of 2014. The usual protective measures are not sufficient when APAAN laboratories are seized. It is necessary to wear chemical protective clothing and, in addition, to follow a special procedure for APAAN decontamination.

According to Vijlbrief, dealing with the illegal production of synthetic drugs and their precursors is a cat-and-mouse game. As a reaction to the measures taken by the police, it can be observed that production and storage facilities are moved constantly and different chemical substances are used.

Kim Nilvall, Detective Inspector at the Swedish National Bureau of Investigation in Stockholm gave a presentation entitled **"The Criminal Arboristic Approach – A method to combat organised crime",** an analytical method to identify strategically important individuals within organised crime groups or networks. Accordingly, the theoretical background, the analytical method, products and additional value with regard to the Criminal Arboristic Approach were outlined.

Organised crime is often described and defined in terms of 'gangs', 'constellations', 'organisations', 'clans', 'OC groups', 'cartels' etc. Therefore, a common approach on how to tackle and evaluate organised crime is necessary. He referred to the one thing we all do have in common: individual contact networks. Criminals contact criminal networks and at different occasions they

get to know new partners there. To understand why some individuals commit crimes together is vital. The Facebook account from one offender (man selling cannabis) was taken as example and his different groups of friends were analysed. Five different clusters of friends upon which a new layer was added were discovered. People that were already known to the police can be detected. This allowed focusing on the 'cluster' with the criminal friends. The structure of an individual contact network was discussed. Social circumstances change the network of each individual, thus they are rather changeable than static. There is also an outer vs. inner circle of contacts, depending on trust towards the different persons. The person whose company is to be sought varies depending on the activity to be undertaken. On some occasions, it might also be wished for an inclusion of persons from the outer circle, such as acquaintances or colleagues. Moreover, it is longed for an avoidance of risks, meaning that people who are not trustworthy will belong to the 'outer circle'. This behaviour can be understood as some sort of risk-assessment. The next topic concerned the extent of the criminal network. An approach of six degrees of separation was established. As Sweden is not a big country, all criminals are connected via few degrees of separation. OC in Sweden can, according to Nilvall, be understood as several individual criminal contact networks that are part of *one* large criminal network. The Criminal Arboristic Perspective (CAP) predicts the effects of crime. Important people in a criminal network are those people who have the ability to keep the network alive and to manage finances as well as developing a criminal repertoire. Nilvall explained how to map a person's contact network and define the inner circle of contacts. The mapping includes e. g. the extent of the contact network, the relationship's degree of closeness and trust, a capacity assessment and a priorisation of strategic persons.

The next topic described the product and additional value of the Personal Analysis Document (PAD). The PAD contains all relevant information concerning an offender. Hence, a tactical report at an individual level is provided. Each of the 21 police agencies in Sweden receives this tactical report and PAD to every 'Criminal of strategic importance' which enhances the operational transparency. Furthermore, Nilvall expressed that the objective is to have an European approach. Norway and Sweden are already following the same approach concerning the PADs. With this approach criminals of strategic importance could be identified all over Europe, as it provides arguments if investigations need to be prioritised.

Thomas Falk, Head of the Swedish Social Insurance Agency's Special Unit against Serious Organised Crime in Hägersten, gave a presentation on "**The new Swedish model – combating benefit fraud in a welfare state**".

Organised benefit fraud is a big problem in Sweden. The Swedish welfare system is financed through income tax and offers various possibilities of abuse. In 2009 several Swedish authorities started cooperating in order to combat benefit fraud. Until then it was not sure whether benefit fraud is only a local or a national and major problem. It was realised that it is a very complex system. In early 2011 the Swedish Insurance Agency launched a national monitoring effort to detect and prevent incorrect payments of attendance allowance, the so-called "Assistance Project". The project is conducted in cooperation with the police, prosecutors, the Swedish Tax Agency and other authorities within the framework of the Regional Intelligence Center (RUC). In 2013, about 40 specially trained investigators worked with control investigation of attendance allowance. One of the investigations were conducted against an assistance company in Södertälje, known for a series of irregularities. The company dealt with assistance to 36 clients and had about 240 assistants employed. Some links to the so-called 'Södertälje-Network' were detected and the case became part of the project "Tore 2", a joint-agency-intitiative against the criminal network in Södertälje with operational backing from the Police. In Södertälje, which is located near Stockholm, there is a community in parallel that has been started by the large Syrian population in the city. It owns most of the city's restaurants, cafes and other cash industries. The parallel society includes its own black economy, its own penal system, banking and lending systems and conducts criminal activities such as drug trafficking and extortion. Part of this criminal network are managers in the Södertälje City Council and a member of parliament. Meanwhile 533 cases of compensation fraud were investigated.

In Sweden, there are many challenges in terms of fraud against the social insurance system, e.g. concerning the dental insurance and the labour market. Criminals commit identity frauds and buy companies which were used as a façade for illicit work and criminal activities.

"The different faces of organised crime in the UK" was the topic of the presentation by **Sarah Groenewegen**, Senior Strategic Intelligence Analyst, Picture of the Threat Team, National Crime Agency (NCA), London. In her speech she gave an overview on the British National Strategic Assessment 2014/2015, an instrument to lead the UK's fight to cut serious and organised crime.

The National Strategic Assessment 2014 is based on intelligence reporting from across the country. It provides the national picture to meet the needs of all stakeholders, including police and government. The aim is targeting serious and organised criminals. In UK, there is no legal definition of OC, which allows the term to be more flexible and adaptable. Generally, serious and organised crime in the UK operates in loose networks. Individuals, pairs or

small groups bring associates and contacts together to work on particular enterprises across multiple crime types. Some serious and organised crime is perpetrated by hierarchically structured groups comprising close associates and/or family members, some of whom are based overseas. The so-called 'Organised group mapping' is prioritising 40–50 high-priority groups. Groenewegen explained that OC also depends on the region of UK. In London for instance, mostly multi-ethnical groups are operating. She presented the dominant organised crime phenomena in the different parts of the UK. The most organised crime criminals are drug traffickers. Groups active in the field of drug trafficking often also get involved in acquisitive crime. Organised acquisitive crime consist of commercial robbery, organised vehicle crime, organised burglary (favoured are metal, jewellery, smart phones) and illegal smuggling of protected wildlife. However, fire arms trade is not a big problem, as it is supply-driven. Most shooting incidents in the UK are perpetrated by urban street gang members. Groenewegen explained that the organised immigration crime and human trafficking, including modern slavery are further relevant criminal phenomena. With regard to people smuggling, criminals profit mainly from facilitating migration. Irregular migrants are often exploited by human trafficking. Modern slavery is divided into the categories of forced labour and servitude. Combating child sexual exploitation and abuse is one of the priorities as there were a lot of cases that became public in the last years. Perpetrators are mostly lone offenders, but they are also operating in groups. Economic crime and cybercrime also characterize the image of OC. Organised criminals using cyber tools 'as a service' and the 'Dark Web' is used in many organised crimes. Another big problem are the organised criminals in prison and under lifetime management. Some high risk individuals continue to offend and coordinate crimes from prison. The majority of those offending coordinate drug trafficking; a few coordinate the supply of firearms. The OC criminals in UK are highly skilled in spotting criminal opportunities and exploiting them. The police therefore cooperates closely with prison services.

The Different Faces of Organised Crime

Stefan Michel

Bundeskriminalamt, Wiesbaden

1   Global impact

Organised Crime, which has become highly complex and dynamic, increasingly networked, more and more sophisticated in terms of technology and more international, causes enormous damage as it is spreading and shows itself in many facets of crime. OC is not only visible in the fragile states of the world, but we all experience the global impact of these forms of particularly socially harmful crime.

Moreover, the global impact of OC is illustrated by various incidents. The killing of journalists in which criminal groups were responsible for the deaths of 141 journalists and media workers in the first decade of this century is one of them. These are mafias, cartels and warlords recycled as traffickers, paramilitaries running rackets, separatist groups that traffic and extort to fund themselves rather than fascist regimes that pose the greatest physical danger to journalists, according to Reporters without Borders in a report entitled "Organized Crime Muscling in on the Media". Furthermore the use and trade in drugs also pictures the global impact of OC especially with regard to the technical development in the past decades. An estimated 183,000 drug-related deaths were reported in 2012, whereas the estimated number of people who inject drugs amounts to 12.7 million. While the internet continues to be used as a means of drug trafficking and illicit trade in precursor chemicals, the use of the so-called "dark net" has been growing. While the overall proportion of drug transactions that take place in the "dark net" is unclear, the value of transactions, as well as the range of drugs available, appears to be growing. The dismantling of one prominent "dark net" site, the "Silk Road", uncovered that the site had approximately 1.2 billion US dollars' worth of total revenue from two to five years of operations. There is evidence of a niche market on the "dark net" for new psychoactive substances as well as for high-quality cannabis, heroin, MDMA and cocaine. One of the "new" faces of OC is mirrored in cybercrime wherein estimations on the losses caused by cybercrime are conducted by a report which tries to attempt the difficult and controversial task of understanding the economic impact of cybercrime, pegging it between 375–575 billion US dollars annually. Regarding the illicit trade and purchase in cigarettes, the World Health Organization (WHO) estimates that 9–11% of the global cigarette market is illicit, yet as shown in an earlier blog: "Illicit

Cigarettes: crime at your corner store" in some countries it is above 50%, and governments could stand to gain at least 30 billion US dollars a year in tax revenues if it were eliminated. Another aspect within the global impact of OC concerns trafficking in human beings. Between April 2008 and October 2010, a criminal organisation recruited more than 20 young, unemployed Hungarian men to come to Canada with the promise of well-paid jobs. Instead, they were exploited and kept quiet by threats and intimidation. The organisation was headed by two Hungarian brothers with a hidden criminal past. They arrived in Canada in 1998, claimed refugee status, acquired knowledge on how to exploit loopholes in the Canadian immigration system and brought members of their extended family to Canada, who then joined their criminal organisation. In this way, they were able to establish what is now known as the largest human trafficking ring in Canadian history. Over the span of almost two years, the clan engaged in a litany of crimes, from human trafficking, welfare fraud, threats, and immigration offences. In addition, the exploitation and orientation towards new markets poses another repercussion within the transnational framework, since East Asia is no longer a peripheral market for drug traffickers, cyber criminals, and human smugglers. The increasing affluence in China, Indonesia, Vietnam, and the Philippines have opened up a market for organised crime figures comparable in value, and larger in absolute population size, than the traditional high-value organised crime markets in Europe and the United States. One estimate notes that by 2025, China's middle class will reach 520 million alone. As East Asia's licit market booms and beckons, so too does East Asia's illicit market, thus transnational criminal groups have moved rapidly to gain an advantage. Another topic possibly also frequently currently covered in the media concerns match-fixing, as the Swiss-based international governing body of the football industry, Fédération Internationale de Football Association (FIFA), has estimated that organised crime brings in as much as $15 billion a year from match-fixing. Criminals have been known to fix matches at nearly every level of the game, from the World Cup to semi-pro and friendly games. The ubiquity of the practice is astounding: more than 60 countries around the world have conducted investigations into match-fixing in the last 2 years alone. With reference to environmental crime, unchecked corruption and sophisticated criminal networks have created an illicit economy in environmental products, which is pushing species to the brink of extinction, transforming thriving rain forests into impoverished wastelands and polluting the environment with toxic waste. The last impact which has global consequences is originated in economic crime. In some cases of economic crime, tax and accounting offences, we are faced with other forms and consequences of organised crime. One would just need to take a look at the exorbitant damage caused by economic crime in Germany, which amounts to approximately 4 billion Euros in 2013, the almost unlimited wide range of investment fraud or the Value Added Tax Carousel

Fraud in connection with emission allowance trade. A case currently conducted in Germany involves as much as 1.5 billion Euros damage to the detriment of the state (source: 2013 police statistics).

2 Characteristics and influential factors

An important question to be raised when examining the faces of OC is to determine the main characteristics of organised crime in the process of change. Apart from the traditional organisational forms of hierarchy of organised crime, the network structures of internationally acting offenders increasingly grow together, for OC has attained a high innovation potential by taking advantage of technological progress. Fixed parameters such as Italian organised crime or Russian-Eurasian organised crime establish themselves in society's structure, hence criminal-geographic areas are created depending on the crimes and offences, so to speak their respective field of activity, and keep on changing. As a result, organised crime is spreading and shows itself in many facets of crime. Another problem is posed as it intermingles with gang crime, becoming more and more difficult to draw an exact dividing line between the two phenomena. This extends the difficulty of making an exact assessment of the situation. Communication structures used by serious criminals are increasingly marked by anonymisation and encryption in the future, also due to the increasing "intertwining" with the internet. These are also the findings of our European partners, as e.g. Europol summed up in its 2013 SOCTA report ("Serious and Organized Crime Threat Assessment"). Therein, Europol estimates that there are 3,600 active criminal groups operating in an increasingly flexible, innovative, global way and in more than one field of crime. What are the according influential factors causing these changes? Legal and factual framework conditions, as a result of the EU enlargement, have considerably changed which also involves a change of the phenomenon of "organised crime" that views and uses Europe as a single market, too. The technological development and internet-based services which are increasingly available throughout the world create new opportunities for offences as well as for new modi operandi. In conclusion, cybercrime in its manifold forms will pose a massive and increasing threat to the EU in the future. Moreover, globalisation and the economic and financial crisis are factors which further the evolution of new forms of organised crime. For example, demographic changes and the economic situation in Africa, the Middle East and in East Asian countries trigger migration movements and provide criminal groups with opportunities to engage in migrant smuggling and trafficking in human beings as well as they enhance the increase of the recruitment potential.

3   Organised crime in Germany

Figure 1: Organised Crime in Germany.

| 620 | 650 | 622 | 602 | 575 | 579 | 606 | 589 | 568 | 580 |

| 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 |

——— Durchschnitt (599 Verfahren)
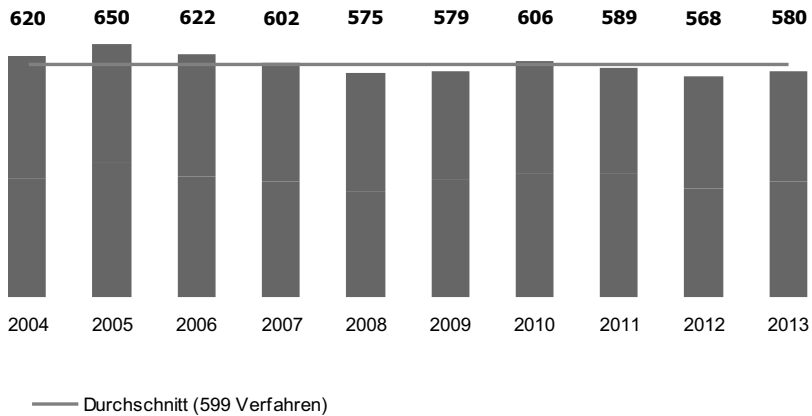
Source: Bundeskriminalamt, Wiesbaden (2014), "Organised Crime in Germany"

In order to fully understand the situation of OC in Germany, one would have to consider the definition of OC by the Bundeskriminalamt (BKA):

> Organised crime (OC) is the planned commission of criminal offences deter-mined by the pursuit of profit or power which, individually or as a whole, are of considerable importance if more than two persons, each with his/her own as-signed tasks, collaborate for a prolonged or indefinite period of time.[1]

As can be detected by figure1, the number of OC investigations conducted in Germany has amounted to about 600 investigations per year for the last 10 years. Moreover, 580 OC investigations were conducted in Germany in 2013 (2012: 568) of which 298 were initial reports. With approximately 600 OC investigations and approximately 9,000 suspects, our German OC situation report does, in fact, not comprehensively describe this form of very serious crime. This does of course not account the number of unreported and unde-tected OC incidents in Germany. The fact that the number of investigations, which has almost been the same for years, does not signify by no means that there have been no changes in terms of quantity and quality. These investiga-tions are recorded on the basis of a strict OC definition which comprises only

---

[1]   Working definition "Organised Crime", passed in May 1990 by the GAG legal authorities/police and serves as basis for the survey.

particularly qualified modi operandi. This means that, apart from the organised and permanent commission of criminal offences, special characteristics are required: Firstly, the use of commercial or business-like structures, secondly, the use of force or other suitable means of intimidation, or thirdly the exertion of influence on politics, the media, public administration, judicial authorities or the business sector (BKA definition of OC). All the other forms of organised commission of crimes are not included, which clearly leaves room for a further expansion of the definition.

Figure 2: Crime on the Threshold of OC.

	OC	Threshold of OC
Investigations	580	Ca. 1,500 to 2,000
Offences	Drugs	Property
	Property	Drugs
Suspects	9,155	Ca. 20,000
Nationality of the suspects	German	German
	Turkish	Romanian
	Lithuanian	Turkish
Dominating nationalities within the groups	German	German
	Turkish	Romanian/Turkish
	Polish	Polish

Source: Bundeskriminalamt, Wiesbaden (2013), "Crime on the Threshold of OC"

In addition to the OC Situation Report, since 2011, the forms of crime on the threshold of OC were accordingly examined. What is meant by crime on the threshold of organised crime? Criminal offences which do not correspond to the complex definition of organised crime and are marked by a high level of social damage can tremendously inflict and seriously impact the public's sense of security and the trust they have in the security authorities. In particular, these include especially gang-type forms of crime and crimes on a commercial basis. We have about 600 OC investigations each year compared to at least 1,500 to 2,000 investigations of crimes on the threshold of OC. Moreover, there are 9,000 OC suspects which are acknowledged in the police statistics, despite there are approximately 20,000 – 30,000 persons engaging in serious and very serious crimes who have – so far – not been reflected by the data collected. Besides, to achieve a maximum of precision in the evaluation and analysis of OC – as in the current OC Situation Report – it is therefore necessary to concentrate the analytic examination on the evolution of orga-

nised crime and the forms of serious and very serious crime which are not included in the traditional definition of OC. The reasons why the aforementioned fact is of such importance lies in the fact that inter alia the quality of investigations dealing with organised crime and crimes on the threshold of organised crime hardly differs which also accounts for the sizes of groups and international orientation of criminals. The number of investigators required for investigations into crimes on the threshold of OC is not much lower.

Law enforcement authorities therefore need to provide almost the same level of resources for investigations into crimes on the threshold of OC. The available data suggests that criminal groups engaging in crime on the threshold of organised crime have firmly established structures and have already established themselves in the criminal markets. Almost all crime phenomena in the field of OC are also found in the field of crimes on the threshold of OC, but in particular property crime on the threshold of OC compared to drugs in the context of OC. Crime on the threshold of OC poses a considerable damage and threat potential: for the damage was an estimated sum of about 460 million in an individual case on the threshold of OC (in 2013). Irrespective of the question of classification, there also comparable challenges the law enforcement authorities face, such as: the increasing internationalisation, the compartmentalisation and the use of modern communication and technology. In closing, one can state that crime on the threshold of OC poses a considerable damage and threat potential.

4   Cybercrime

This chapter is occupied with OC in the process of change and therein the role of cybercrime. The causes of the changes in the crime situation and hence OC and forms of crime on the OC threshold are going to be outlined. However, one aspect has to be highlighted in this context: Namely the fact that the technological development has created a completely new quality of crime commission and opportunities for crime. The internet serves as the perfect platform for committing offences because it is quick, anonymous and globally networked. In addition, the number of offences which use or target information, as well as communication technology continues to increase although the number of OC investigations in this field of crime appears to be moderate**. The number of OC investigations does not reflect the threat potential but shows the difficulties the investigating authorities are forced to face. Sometimes we deal with different criminal groups who are independent of each other and offer individual elements for the commission of crimes as a service for several different groups of offenders, either simultaneously or within the same period of time which could be regarded upon as a traditional division of tasks. Furthermore, offender groups usually share information via

anonymised communication channels and use a special "cyber language". Therefore, innovation cycles of modi operandi are becoming shorter: offenders are more flexible, keep looking for new gateways and use every technological possibility for their criminal purposes. More importantly, national borders are irrelevant because offenders' whereabouts, crime scenes and the places where success is achieved are not the same. Evidence can no longer only be detected at the crime scene but rather is transferred to a cloud which has a considerable impact on our investigative options. Regarding communication, data gathered by the BKA in the years 2012 and 2013 have shown that in 67 percent of all cases it concerned organised crime. Moreover, agreements were made among the offenders regarding the use of encryption, whereby several encryption services were used in more than 40 percent of the cases. Furthermore, it could be stated that the mobile internet results in "nomadic" user behaviour. The market has moved towards mobile internet communication in recent years which means that we have very limited access to offenders' communication. As the volume of digital information is enormous, increasing amounts of data are detected in the course of investigations. Even now, we struggle to cope with seizures of data in the range of 1 terabyte up to 1 petabyte. This makes data processing and evaluation a highly demanding task.

5   Traditional OC groups

The focus now shifts to some specific faces of OC, whereas it is important to note that the description is not complete and only serves as an example. Initially, the focus lies on the different "faces" of OC on which we have concentrated our efforts for years, namely the traditional organised crime groups. There are numerous examples of organised criminal groups who fulfil social functions and are marked by a particular sense of togetherness of their members and the commitment to mutual consideration as for instance: Outlaw motorcycle gangs such as the Hells Angels, Bandidos, Thieves in law (*vory-v-zakonye*) of the former Soviet Union, the Italian Mafia organisations such as the Sicilian Cosa Nostra or the Calabrian 'Ndrangheta, the Chinese Triads, the Japanese Yakuza groups and the drug cartels in Latin America. Besides "traditional" OC, however, nowadays there is an increasing number of criminal groups who intend to make maximum profits and further invest the illegal money, and therefore a sense of togetherness of their members or common roots is no longer of importance to them, for they are also marked by a higher level of heterogeneity. Altogether, the dividing lines between organised crime and crime on the threshold of OC are blurred.

5.1 Outlaw Motorcycle Groups

Traditional examples from Germany on which we have been concentrating our efforts are outlaw motorcycle groups (OMCG). In Germany, we have been dealing with approximately 9,000 members of outlaw motorcycle groups who are organised in ca. 650 chapters/charters. The four major outlaw motorcycle gangs are: Bandidos MC, Gremium MC, Hells Angels MC, Outlaws MC and furthermore, the Satudarah Maluku MC (SMMC) from the Netherlands and the Mongols MC (MMC) from the United States which both have increasingly become noticed and try to establish themselves in Germany. The four major motorcycle gangs are characterised by their members' particularly high delinquency. Outlaw motorcycle groups are marked by a hierarchical structure, compartmentalisation, an own set of bylaws and high propensity to violence. Violent offences including serious bodily harm and homicide offences between warring outlaw motorcycle groups, mostly committed in public places, are not uncommon. Moreover, violations of the drug and weapons legislation are often detected. A total of 337 investigations was conducted in Germany in 2013 (2012: 365) (approx. −8%) which were linked to outlaw motorcycle gang crime in accordance with the definition. Further, 858 suspects (2012: 778) were identified (approx. +10%). The outlaw motorcycle groups' main fields of activity in Germany were violent crimes (49%), drug trafficking (16%) including violations of the Pharmaceuticals Act, violations of the Weapons and the Explosives Act (11%) and other criminal offences (24%) such as crime associated with nightlife. The "outlaw motorcycle gang crime" phenomenon is of considerable importance and is therefore given a great deal of attention by the law enforcement authorities as it has become more multi-layered and complex and no longer allows gaining a clear overview as OMCG are joined by new members and supporters regularly. It is not only the established traditional outlaw motorcycle groups who have been in the focus of attention, but also numerous newly formed supporter clubs, groups similar to outlaw motorcycle gangs and "street gangs" pose an additional potential threat with regard to conflicts among each other and with regard to the established groups. OMCG are internationally networked and partly co-operate with other OC groups, which is proven by the fact that Outlaw motorcycle gangs have been found to exist in all EU member states and are consequently of significance at a European level.

5.2 Russian-Eurasian organised crime

Regarding Eurasian Organised Crime (REOC) it can be noted that its structures have firmly established themselves in Germany over the years and Russian Eurasian crime sees itself as a parallel society with its own systems of

values and norms. The ideology of the "thieves in law" has its origin in the former Soviet Union's prison camps (GULAG) in the 1930s. It has meanwhile been rooted in parts of the Russian speaking community in Germany – about 4.5 million people in total – and it particularly appeals to some people of the young generation who feel excluded from German society. The spreading of this ideology is particularly evident in German prisons where about 4,500–5,500 prisoners of Russian descent/Russian speaking prisoners are detained permanently. The use of symbols is of high importance to the thieves' ideology which is also reflected in their tattoos. What is the structure of Russian-Eurasian OC? The main feature is a hierarchical, military-like structure, which is shown here as a pyramid. The individual command levels are strictly separated from each other. The highest authority figures are at the top of the pyramid, predominantly the traditional "thieves in law". They are judges within their jurisdiction and settle disputes in the criminal scene. Furthermore, they are crowned by other "thieves in law" as part of a ritual and accepted by the brotherhood. Interpol estimates that there are currently 950 crowned "thieves in law" throughout the world. "Thieves in law" exert their regional influence through residents (Russian "Smotrijaschi"), who in turn monitor the work carried out by the individual brigades and gangs in the thieves' sphere of influence. Another significant element of Russian-Eurasian OC structures are the so-called thieves' cash registers (Russian "Obshak" system), into which each sub-organisation has to pay a certain amount of money. On the one hand, "Obshak" serves to finance criminal offences and corruption, and on the other hand, it is a social fund intended to support imprisoned members of the organisation. What is the situation in Germany? If we just look at the surface, the situation is calm. Russian-Eurasian OC currently does not play a particular role in media coverage and hence in public perception. If we take a closer look, however, we see how firmly these structures have established themselves and that Russian-Eurasian organised crime is active in almost all fields of crime, such as drug trafficking, money laundering, economic crime and extortion as well as violent and capital offences. At the present time, investigating authorities in Europe devote particular attention to Russian-Eurasian offender groups whose actions are mainly discernible as shoplifting and theft by breaking and entering in the context of organised property crime and which cause enormous economic damage. In particular, Russian-Eurasian organised crime is currently in some sort of consolidation phase after fights for predominance in Europe, in the course of which much blood was shed. We expect REOC structures in Germany – also compared to other ethnic groups – to be more effective and more assertive than before. Information about the situation in Russia leads to the conclusion that a new REOC leadership has come to terms with the state administration and is also more socially adapted there. Much suggests a mutual infiltration of the politi-

cal sector, business life and the criminal community in Russia, and this situation will also have an impact on Europe. The dangers posed for Germany are in particular perceived to be the high financial damage and removal of criminal proceeds from Germany and the return of criminal proceeds as investments at a later stage, the firm establishment of a subculture in Germany's population of Russian descent, the security threat in prisons as a result of subcultural behaviour, the gradual evolution of a favour and corruption culture modelled on "Russian business patterns" and the possibility of influencing markets (for example the real estate market) and opening ways of political influence.

5.3   Italian organised crime

Another traditional OC group is pictured by the Italian Mafia, which continues to regard Germany mainly as a safe haven and place of retreat. During the past 15 years, a total of 244 OC investigations were conducted into Italian OC groups. The peak was reached when six murders were committed in Duisburg in the year 2007 which were evidence of Mafia crime structures in Germany. A joint working group was established as early as the mid-1990s which made it possible to obtain quite a precise picture of Mafia members' presence in Germany. This also led to the arrest of 314 Mafia members in Germany between 1995 and today for different crimes, including murders committed in Italy. Since the murder of six persons in Duisburg in 2007, a German – Italian Task Force has also been set up which is aimed at an optimised police information exchange and closer operational co-operation. At the present time, approximately 550 suspected Italian OC members are living in Germany, of whom 293 can be linked to the 'Ndrangheta, 108 can be linked to the Camorra, Cosa Nostra/Stidda and 18 to the Apulian OC.

5.4   Gang-type crime and crime on a commercial basis

Attention is moreover drawn to other forms of crime which – as supposed widespread offences occurring in great numbers – are to be attributed at least to gang-type crime and crime on a commercial basis and in some areas are also embedded in internationally operating OC structures. As an example, it is elaborated on organised fraud committed by call centres. Fraud offences have come to notice for several years where initial contact is made by call centres predominantly based in Turkey. The callers make promises of prizes in return for advance payments or create threat scenarios and make unauthorised claims. In Germany, approx. 1 million victims have suffered damage of approx. 120 million Euros. The victims are mainly elderly persons

and the number of reported cases is estimated to an amount of 10 percent at maximum. The offender structures act in an organised way and across borders. They proceed based on a division of tasks with the aim of concealing their actual responsibility. The offenders in the call centres are trained to talk to people and are well and professionally prepared to do telemarketing. They successfully induce their victims to send money on several occasions. The offenders manipulated communication via Voice over IP (VoIP) in order to conceal the fact that the calls were made from Turkey – the technology used by them makes it difficult or impossible to carry out effective police investigations. Altogether, the dividing lines between organised crime and crime on the threshold of OC are blurred here, in particular in the field of supposed widespread offences which are embedded in organised crime structures operating at international level.

5.5   Structural property crime

An additional example is structural property crime in the field of daytime burglary of dwellings committed by travelling groups of offenders. In Germany, there was a decline in the number of burglaries of dwellings until 2006. Since then, the case numbers have been rising steadily. An analysis of the structure of suspects has revealed that the increase is largely due to offenders and groups of offenders from South East and Eastern Europe, adding the trend in the European neighbouring countries is similar. The proportion of non-German suspects has steadily increased from 19.8% in 1999, to 31.1% in 2013 (5,497 from 17,703 suspects). Over the last four years there has been an increase of 43%. The largest group of non-German suspects is made up of Turkish nationals who have a similar crime scene-dwelling-relationship as the German suspects and are therefore first and foremost local-regional offenders. The proportion of Serbian, Romanian and Polish nationals has increased disproportionately. As the crime scene is often far away from where they live, namely abroad, they are called "travelling offenders", for they travel to Germany from abroad to commit crimes. Some remain in Germany for a few weeks or even months in order to carry out burglaries of dwellings or commit other crimes. They often use the services of so-called "residents". As a rule, these are fellow countrymen who are points of contact and can organise vehicles, apartments and documents. Should someone get arrested, they also hire a lawyer. These "residents" can also say where suitable buildings/residential areas are and can sometimes help to dispose of the stolen goods.

5.6   Ethnically closed clan structures

In different German cities, the establishment of ethnically closed clan structures and their connections with organised crime structures involving more than 1,000 family members was observed. These are extended families of Arab descent, concerning criminal activities, their main areas of crime include smuggling of and trafficking in hard drugs such as heroin/cocaine, crimes relating to the red-light scene (trafficking in human beings, illegal gambling), racketeering, weapons trafficking and the facilitation of illegal immigration. Moreover, honour and blood vengeance related offences, rooted in their culture, are not uncommon. Common features of these clan structures are: The social structure of their community of origin with its strict division into patriarchal tribal hierarchies is also maintained in the host country as well as the strict adherence to, and enforcement of archaic tribal rites, which in part are diametrically opposed to the social code of conduct of Central European host countries and in many cases trigger cultural conflicts where considerable violence is used based on the code of honour existing in their home countries. Disputes within the clans or between the clans are settled by the "justice of the peace" or "Sheikh". Another feature is the marked isolation from the outside. These mechanisms described make police investigations considerably difficult.

6   Conclusion

Summing up, organised crime is not an invisible danger, for it uses lawful economic structures, affects competitiveness, creates structures of corruption, undermines institutions, damages the environment, exploits weak or even failing state structures, fuels conflicts, and may even pose a threat to life and limb. Organised crime has many different faces and forms: we no longer deal with organised crime in the traditional sense – widespread crime as a phenomenon at a local level can now be the result of globally organised criminal networks. OC and gang crime diffuse so that it is more and more difficult to draw an exact line between the two phenomena. The technological development poses new challenges to us as we can see the rapid development in the field of cybercrime: the internet as an instrument of and opportunity for crime. Proven investigative tools to detect suspicious circumstances and gather evidence in the fight against very serious forms of crime are becoming less significant. When recovering and analysing evidence we are confronted with considerable problems resulting from the big data issue which leads to highly complex and very resource-intensive investigations. In the light of the issues above, we have to define our position in the fight against organised crime. An initial step involves a description of the situation which abandons the narrow point of view and strict definitions of fields of crimes and describes the threat

potential in a realistic way. In this context, we should bear in mind that Europe and, in particular the European Union, constitutes a common criminal-geographic area and a "criminal market", too. This is taken into account by Europol's Serious and Organized Crime Threat Assessment (SOCTA). The SOCTA should, however, be further developed towards a uniform understanding of organised crime in Europe. In this connection, adjustments and modifications of the suppression strategy should be considered – with regard to criminal law and tactical aspects – both at national and international level. An effective fight against organised crime is only possible in concert and by networking with partners of the European and international security architecture as well as in co-operation with the business sector, scientific world, society and the political sector. In furtherance of a holistic concept, new alliances must not be a taboo, since organised crime is not exclusively a problem the security authorities face – it concerns the whole of society.

Understanding the Emergence, Mobility and Specificity of Georgian organised Crime Groups in Europe since 2006

Gavin Slade

Free University, Berlin

1   Introduction

Recently there have been a number of Europe-wide crackdowns on Russian speaking organised criminal groups. In 2010, Operation Java netted 69 people reported in the press as 'Russian mafia'. They had been operating particularly in Spain and France. In 2013, 18 more people were arrested in a variety of European countries including Italy, Lithuania and Hungary. In 2015, in France, 33 people were arrested for engaging in organised criminal activity focused on low-level robberies. In all of these cases, on closer inspection a great many of the arrestees were not ethnic Russians but Georgians or Georgian nationals. Where Spanish police worry about money laundering, Austrian, Germans and French report organised burglary, shoplifting and carjacking. In Greece, there is some evidence of labour racketeering activity among the country's Russian-speaking, Pontic Greek population and Georgian immigrant population, totalling up to more than 300,000 people.

This article seeks to understand the emergence of a 'Georgian organised crime' problem in Europe. The paper argues that we should be careful not to fall into the 'ethnicity trap' (Tilly 2006) and see the Georgians as the next in a long line of 'threats' to European Union societies, following Russians, Chechens and Albanians in the past. The paper does, however, show how recent political developments in Georgia have caused transplantation of particular forms and structures of organised crime into Europe that are particularly problematic for law enforcement. The paper, based on research conducted by the author on the Georgian mafia over the past 8 years (see Slade 2013), argues that local factors in Georgia led to the emergence of particularly adaptable criminal groups, more than in other post-Soviet countries. It further argues that local practices that originally emerged in prison are now being used in a European context to structure organised criminal activities. I first turn to the Georgian context and how political change has caused criminal transplantation.

2   Anti-Mafia in Georgia

In November 2003, widespread and peaceful protests unseated incumbent President Eduard Shevardnadze in Georgia. Fraudulent parliamentary elections had been the trigger for regime change that became known as the Rose Revolution. In 2004, fresh elections brought to power the former Justice Minister, a young reformer called Mikheil Saakashvili and his United National Movement. One of the main platforms Saakashvili was elected on was to clean up the endemic corruption and organised crime in the country after the turmoil of the 1990s. Building on contacts and policy exchanges with the anti-mafia Sicilian Renaissance movement as well as the know-how of Italian prosecutors sent to Georgia by the EU to support legal reform, Saakashvili's government prepared an all-out assault on organised criminal structures in Georgia.

Such structures existed within the cultural framework of Soviet penal subculture, known as the *vorovskoi mir* or thieves' world. The main actors within this subculture are known as thieves-in-law ('law' as in a code of honour) or *vory-v-zakone* in Russian. This title emerged in the Soviet labour camps in the 1930s to denote an elite prisoner leader. This elite was drawn from all ethnicities. By the 1960s and 1970s *vory-v-zakone* were acting outside prison, racketeering the second economy of the Soviet Union. For reasons that are not entirely clear, Georgia became the biggest producer of these actors. By the collapse of the Soviet Union, it was estimated that 33% of all *vory* were from Georgia, even though this tiny republic in the south of the Soviet Union made up only 2% of the Soviet population. In popular discourse, Georgia in some ways occupies the same place for the Soviet Union as Sicily for Italy: both Southern regions supposedly inhabited by hot-headed people driven by traditional customs and chivalric notions of honour.

Georgia did not produce so many *vory* for cultural reasons however. Like Sicily, the lack of a functioning state and a long history of foreign occupation, most likely gave rise to actors with the violent capital to exploit opportunities in the market for protection. This market grew to remarkable levels in the second economy of the Soviet Union. Studies of illicit trade in Soviet times show that the second economy was largest proportionately in Georgia, Azerbaijan and Uzbekistan. Here the strength of the state and criminalisation of entrepreneurial activities gave rise to a demand for protection among those engaged in black markets. Archival data from Georgia show that mafias headed by *vory* moved to combine with second economy actors in the 1980s. The market for protection grew to even larger proportions in the 1990s however. Other than Tajikistan, Georgia suffered the worst state collapse of any former Soviet state. Two separatist wars, one civil war and revolution as well as detaching from the Soviet joined up economy saw over 80% of Georgia's

industrial production wiped out. With a weak state, property rights in the new market economy were left unprotected. Trust in trade could not be guaranteed. Disputes could not be resolved. Once again, all the evidence points to *vory* operating as sellers of protection and dispute resolution services to fledgling businesses, traders and even politicians.

Together, the huge second economy, followed by an extreme example of an unprotected market in a weak state context, are the key elements leading to Georgia producing so many violence-wielding mafia actors. Culture plays little role other than in framing the form that these mafia actors took and the presentation of themselves within Georgian society. Data from Georgian police shows that one particular region, Imereti and the city of Kutaisi, in the west of Georgia, stands out in terms of producing *vory*. There is nothing culturally distinct about Kutaisi in Georgia thus other reasons must be found for its prominence. Today in EU countries it is precisely groups loosely tied to *vory* from Kutaisi that have been arrested, though other regions of Georgia and the capital Tbilisi are also represented.

The anti-mafia campaign was set in motion by Saakashvili's government in December 2005 with a new Law on Organised Crime that targeted these professional criminal actors – the *vory* – specifically. The law outlawed membership of the thieves' world and the status of thief-in-law. Penal reform removed *vory* from the bulk of prisoners. Asset seizure was carried out. The law was targeted and at the same time cast a wide net. As part of zero tolerance policy, the prison population increased sharply, from 6,000 in 2003 to 24,000 in 2010 representing the fourth biggest prison population per capita in the world by that time. In a victimisation survey conducted in 2010, 70% of respondents said that the influence of the *vory* had 'significantly decreased' suggesting that the anti-mafia campaign had been relatively effective (Slade 2012). As noted by many at the time, a lot of the *vory* in fact left the country or cut ties with Georgia in the wake of the new laws and policies.

The Georgian state policy then is a big cause of the recent panic around Georgian organised crime in Europe. As has been shown in academic studies, push factors such as state policies or internecine conflict are common factors to cause movement of organised crime, rather than strategic expansion (Varese 2011). However, it should be noted that many Georgian *vory* had left the country before the 2005 policy due to the turmoil and economic collapse in the country in the 1990s. These *vory* mainly went to Moscow and other parts of Russia, some became very influential taking up positions in the trade in narcotics and moving into legitimate business. These Georgian criminal actors too have found interests in Europe in the 2000s. For example, Spain became a main destination for money laundering, as it did for corrupt Russian business.

It is also important to note the difficulty of defining the issue of *vory* and Georgian immigrants today in the EU as one of 'Georgian organised crime'. For one thing, many of the groups uncovered in Europe are not Georgian at all but come from a wide range of ethnicities and nationalities and can include Armenians, Azerbaijanis, Russians and citizens of the Baltic States. Secondly, as a related matter, Georgians operate utilising coordination across Russian-speaking groups sharing common interests, language and cultural understandings rather than ethnicity. Thus, it is important not to fall into an 'ethnicity trap' in thinking about the policing of a new wave of crime that appears to come from Georgia.

Instead, as opposed to ethnicity or interpersonal networks, I will argue below that focus is better placed on the investment made by migrants in informal institutions and structures that enable coordination between Georgian criminals as well as members of other Russian-speaking organised criminal groups.

3 Practices facilitating Coordination of 'Georgian organised Crime' in Europe

The Soviet Union was a highly punitive state that produced millions of prisoners and ex-prisoners who developed and proliferated a well-articulated penal subculture throughout the country. This subculture fostered a range of understandings, practices, rules and informal institutions that, during Soviet times, enabled Soviet prisoners to alleviate, to the greatest extent that they could, the pains of imprisonment. Prisoners, living in open camps, interacted frequently but produced ways to reduce conflict, control violence and trade what little they had. Informal governance institutions spread across the entire, huge space of the Gulag as information flowed with prisoners and through corrupt prison administrations. Prisoners could transfer from prison to prison and find a familiar set of rules and practices in each one. Hard won status markers were maintained even during transfer.

Key elements of this system of prisoner governance and coordination, was the common pooling and distribution of resources, known as the *obshchak,* and decision-making mechanisms known as the *skhodka*. Strict hierarchies and social boundaries were also maintained. A social structure marked by status distinctions was utilised to monitor and control group formation, the spatial segregation of prisoners and their social interaction. At the head of these hierarchies were the *vory v zakone,* as already mentioned. Below them, a number of authoritative prisoner statuses existed. One important one was that of the 'overseer'. Just as the name suggests, the primary activity of these prisoners was to monitor the other prisoners on behalf of the *vory*. Overseers

watched over dormitories, barracks, punishment cells, the playing of card games, the collection of the *obshchak*, even the prison hospital. A uniformity and order to prison life meant that not all prisoners were opposed to the structure imposed by the thieves' system.

What does this Gulag history have to do with the spread of Eurasian organised crime, whether Georgian or not, in the European Union today? Simply put: Russian-speaking organised crime today utilises practices that used to aid mobility, stability and coordination of collective action across Soviet prisons. The practices and understandings that emerged in the Gulag have been perfectly well adapted to serve as mechanisms for establishing trust over long distances and in new environments for organised crime. Georgia, for reasons explained above, produced a disproportionate amount of *vory,* or the top-level prisoners, who frame their actions in terms of that Gulag subculture. Thus, it is no surprise that Georgian organised crime perhaps more than other Russian-speaking organised crime, utilises the old prison mechanisms for enabling expansion.

There are two ways in which this works. Firstly, we have observed high-level *skhodki* occurring in a variety of places in the last years including in Barcelona, Athens, and Dubai. Here decisions are made about spheres of influence, disputes are resolved, people are assigned tasks, overseers are appointed, and new *vory* are, in the criminal jargon, 'crowned'. The *obshchak* is utilised as a criminal corporate entity where resources and profits are pooled, and dividends paid out. The *obshchak* exists on many levels but funds invariably funnel upwards. Transfers between *obshchaks* can be made on trust without actual physical movement of cash, similar to a *hawala* system of money transfer.

Secondly, the penal subculture of the *vory* became so widespread, and particularly in Georgia, that even Georgian migrants who have no interest in the subculture would have a knowledge of who the *vory* are, how they operate and what rules must be adhered to. Thus, whether Georgian women in the care industry in Athens, or unemployed asylum seekers in Germany, Georgian nationals can be abused by a pervasive system that seeks to extract money or labour from them. Furthermore, this system may also be something that migrants wish to utilise for protection or as a source of illicit income. There is evidence for example of money transfers operated by Georgian criminal groups out of Athens, provided for those working as illegal migrants. The symbolism and reputation of the *vory* and the Gulag practices that facilitate their coordination and movement are very recognisable to citizens of post-Soviet states and among Georgians maintain a particular significance and salience due to the depth of *vory* penetration in Georgia.

4   What is to be done?

In conclusion then, police work in tackling this latest manifestation of 'eastern European organised crime' should not look to understand Georgian or other Russian-speaking groups as having some ethnic peculiarities or specificities. Instead, Russian-speaking organised crime is defined by a set of practices and organisational features that have been adapted from one of the largest systems of incarceration in world history, the Soviet Gulag. By focusing on the ways in which individuals, wilfully or otherwise, may become locked into a system that aims at coordination and pooling of criminal proceeds at a high level within a particular, understandable criminal culture, police work as well as ameliorative social policies towards migrants, can help tackle the problem of organised crime coming from the former Soviet Union. Georgia is a particular case of this in the present day. It is a country where various sections of the population embraced the penal subculture and its leaders to a greater degree than anywhere else in the Soviet Union. It is also a country where, due to its previous government's harsh and successful anti-mafia policy, many people with criminal connections and an admiration for *vory v zakone* have been pushed abroad.

Finally, the prisons of Europe are full of foreigners. A simple comparison shows that foreign nationals are as disproportionately represented in the prisons of Europe as African-Americans are in the US (Waquant). In the countries of southern Europe such as Greece or Italy, the percentage of foreigners behind bars can be over half the prison population. In Germany, numbers of foreigners in prison have also risen sharply. This can be for many reasons, including sentencing guidelines or judicial procedures. Foreigners are less likely to be given bail for example, for objective reasons, and thus make up a large proportion of pre-trial detainees. In any case, studies show that the increase in the diversity of people in prison has also led to a decline in trust. In such a situation, demand for governance mechanisms and informal structures to aid social interactions can emerge. Some evidence suggests that foreign nationals may import readymade penal subcultures into prisons in other countries. While this can be a good thing for prisoners, enabling trust, mutual support and healthy social connections, the case of Georgia and the former Soviet Union suggests that informal institutions in prison can also be used as coordination mechanisms for the goals of organised crime both inside the prison and on the outside. Thus, it is necessary to consider a programme of research into prison life in a multicultural context in Europe and the degree of porousness of prison walls in allowing prisoner-created institutions to inform and facilitate the trust and coordination needed for the expansion of organised crime.

Bibliography

Slade, G. (2012). Georgia's war on crime: creating security in a post-revolutionary context. In European security, Vol. 21, No. 1, pp. 37–56.

Slade, G. (2013). Reorganizing Crime: Mafia and Anti-mafia in Post-Soviet Georgia. Oxford: Oxford University Press.

Tilly, C. (2006, September). Avoiding the ethnicity trap. In Sociological Forum, Vol. 21, No. 3, pp. 523–525. Kluwer Academic Publishers-Plenum Publishers.

Varese, F. (2011). Mafias on the move: How organized crime conquers new territories. Princeton University Press.

Wacquant L. (1999). 'Suitable Enemies': Foreigners and Immigrants in the Prisons of Europe. Punishment & Society, No. 1, pp. 215–222.

Organised Crime and Corruption in the Context of Development

Ugljesa Zvekic

Global Initiative against Transnational Organized Crime

The international community has become increasingly aware of the extent to which organised crime and corruption serve as spoilers of sustainable development. This realisation has been enshrined in a number of United Nations seminal reports such as the report of the United Nations (UN) Secretary-General, "In Larger Freedom," (2005); the 2010 "Keeping the Promise" report of the Secretary-General as well as the World Development Report (2011).

While organised crime and corruption are not new phenomena, their spread, impact and forms in the modern world are unprecedented. The effects of organised crime and corruption are being felt in developing and developed nations alike.

In fragile states and in situations of peace building and state consolidation, organised crime and corruption are increasing threats. In a number of theatres, criminal groups and illicit flows have been proven to fund conflict and perpetuate violence and insecurity.

Organised crime and related corruption have been observed reaching into the highest levels of government and the state, impacting stability, governance, development and the rule of law. Even in what are considered strong and prospering states, organised crime and corruption have serious corrosive effects.

Poverty and inequality are associated with increases in organised crime and corruption, not least in relation to human trafficking, smuggling of counterfeit goods, the production of illicit crops, and everyday extortion and bribery.

Moreover, there is a growing body of anecdotal evidence of the myriad ways organised crime negatively impacts the environment, such as by destroying biodiversity, threatening key species, or reducing the sustainability of ecosystems. In dealing with fisheries and marine ecosystems, addressing the problem of large-scale illegal fishing has become more urgent than other research priorities. In fields like sustainable forestry, a substantial proportion of development assistance is being diverted through illegal logging. Drug trafficking has also been a cause of deforestation of large sections of land.

While organised crime and corruption importance is recognised in the creation of Target 16.4 "By 2030 significantly reduce illicit financial and arms flows, strengthen recovery and return of stolen assets, and combat all forms of organised crime" is welcomed, what the findings of this study show is that the impact of organised crime on development is extensive and diverse. Organised crime and corruption cannot be viewed as separate development challenge to be addressed in isolation. Rather, an effective response calls for the recognition that organised crime and corruption are intrinsic elements to nearly every development challenge, and must be interwoven throughout broader development response frameworks. This is the response requirement that this paper seeks to address. The failure to account for and address fundamental aspects of organised crime and corruption will directly impede and perhaps threaten existing gains in social and economic development.

As the issues of organised crime and corruption expand beyond the sphere of justice and security into a mainstream development concern, the definition of those charged with responding to it needs to be similarly expanded. While political will, capacity building and engagement with state institutions remain essential, a range of other actors and stakeholders needs to be brought to the table. Criminal groups have shown impressive capacities to understand the value of legitimacy through economic and social means, and this needs to be matched by similar efforts by governments, civil society and the private sector.

To achieve a wider buy-in, sensitisation to organised crime and its impacts is still required for practitioners active in the development domain, as well as in related debates on conflict and fragility, human rights, health and the environment. The issue is neither well-understood nor has it become mainstream. Contributing to the limited response to date is the reality the development community lacks a rigorous framework around which to understand, analyse and respond to organised crime.

The renewal of the Sustainable Development Goals (SDG), as a universal development agenda, is a key opportunity to sensitise development actors to organised crime and corruption and ensure that it is built into the development lexicon, so that development actors are able to identify organised crime when it affects the achievement of their mandates. In addition, they should feel equipped to bring development approaches to bear to mitigate the impact of crime on human security, the environment and on development, and to address the root causes.

There are five development impact areas, illustrated in the diagram below, in which organised crime arguably does the most damage.

A second area earmarked as a priority was to focus on illicit financial flows including a target to "reduce illicit financial flows and tax evasion, and increase stolen-asset recovery by $x." While illicit financial flows are, by their very nature, intended to remain covert, in many ways they are the most concrete and quantifiable of the indicators of corruption and organized crime. As the objectives of corruption and organised crime are quintessentially in the realisation of profits, the ability to launder the proceeds of crime into legitimate markets is a critical part of the criminal economy chain. Illicit financial flows have been valued at up to US$1.7 trillion a year, most of which is derived from illicit trafficking in drugs, arms or humans; the diversion of state funds (including natural resources, embezzlement, tax avoidance and corruption), and trade mispricing. The scale of illicit flows have, in some cases, been used as a proxy for the overall rate of organised crime, and are a useful indicator of the likely impact of organised crime on state capacity to deliver services. Despite the scale of illicit financial flows that have been registered, the overall global trade architecture has neither the policy framework nor the systematic protocols to engage.

1 Addressing Organised Crime and Corruption in Sustainable Development Goals

In this section, each of the proposed SDGs is reviewed, as well as relevant targets under the goal. A brief introduction will highlight the direct and indirect impacts of organised crime on the potential for achievement of the goal and targets. In many cases a short case study is provided to illustrate the way in which organised crime can serve as a spoiler. Following this, a short commentary on recommended responses and modes of implementation is provided. A commentary of the implementation modalities is also provided, as it relates to mitigating the impact of criminal spoilers on development targets. When available, relevant modes of implementation provided under the Goal are specifically addressed.

2 Goals at Risk

The four goals identified here – health (Goal 3), marine environment (Goal 14); terrestrial environment (Goal 15) and peace and governance (Goal 16) – have been red-flagged as the primary SDG goals that are directly impacted by organised crime and corruption. In the case of each, the overall SDG goal cannot be achieved if organised crime and corruption are not addressed.

Goal 3:	Ensure healthy lives and promote well-being for all at all ages
Goal 14:	Conserve and sustainably use the oceans, seas and marine resources for sustainable development
Goal 15:	Protect, restore and promote sustainable use of terrestrial ecosystems, sustainably manage forests, combat desertification, and halt and reverse land degradation and halt biodiversity loss
Goal 16:	Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels

3 GOAL 3: Ensure healthy lives and promote well-being for all at all ages

Organised crime will affect the achievement of Goal 3 in a number of direct ways, including through increased narcotic drug usage as a consequence of drug trafficking, the production and trafficking of falsified and substandard pharmaceutical products, and increased rates of tobacco usage due to illicit cigarette trafficking. Moreover, some countries have reported the infiltration of organised crime groups directly into the healthcare industry, and as perpetrators of health-care insurance fraud, which reduces the viability of the entire national health-care industry, and increases the costs of healthcare and health insurance for the general public.

In particular, the impact of narcotic drug use has exerted considerable pressure on the health systems of many countries in both the developed and the developing world, many of which are ill equipped to deal with the burden of drug prevention, treatment and care. The use of injection drugs, such as heroin, cause in an increase in the rate of transmission based diseases such as HIV/AIDS and hepatitis, among others. This is particularly acute among certain populations: low income, marginalised and poverty stricken, lesbian, gay and transgendered communities, and prison populations. Furthermore, drug addiction is frequently linked to the recruitment and perpetuation of forms of human trafficking, in particular for sexual exploitation. Healthcare systems similarly struggle under the increased burden of dealing with the victims of violent crime, which frequently results from organised crime and drug trafficking.

Beyond the direct impacts, a multitude of indirect links can also be made. Increasing levels of grand corruption related to organised crime have resulted in weakened service delivery and the diversion of funds away from government programmes, including in the health sector. Similarly, the need to increase ex-

penditure on security priorities to control organised crime, such as law enforcement and border control, can divert limited government resources away from investments in social services like health and education. Other consequences of organised crime include health worker absenteeism. Underpayment of health workers, who may already have little incentive to abide by the rules and carry out their work, can result in increased levels of absenteeism, as well as the diversion of medical supplies onto the black market. In turn, the erosion of the health sector can diminish public confidence in the government as a whole.

3.1 Relevant targets under goal

– 3.3: By 2030 end the epidemics of AIDS, tuberculosis, malaria, and neglected tropical diseases and combat hepatitis, water-borne diseases, and other communicable diseases.

– 3.5: Strengthen prevention and treatment of substance abuse, including narcotic drug abuse and harmful use of alcohol.

– 3.7: By 2030 ensure universal access to sexual and reproductive health care services, including for family planning, information and education, and the integration of reproductive health into national strategies and programmes.

3.2 Modes of Implementation

The recommended response under Goal 3 is very limited, focusing only on reduction in tobacco consumption, and begs the question of why other control mechanisms – such as ratification and implementation of the Drug Conventions and Protocols – are not put forth.

It is strongly recommended the tools utilised in achieving Goal 3 are expanded to include a broader array of issues and resources. In particular, within the framework of a goal to improve health and well-being, emphasis should be given to reducing drug trafficking and human trafficking, and enhancing the capacity of groups and communities vulnerable to these pernicious threats. A wide range of tools and resources exist both at the policy and programmatic level in this regard. There is also a wide range of lessons to be learned and opportunities for capacity development through shared learning or south-south exchange should be encouraged.

In addition, it is recommended responses ought to contain strong prevention components. The UNODC estimates that for every dollar spent on prevention, at least ten can be saved in future health, social and crime costs. A prevention based approach is mandated by the three international drug conventions and their subsequent protocols: the Single Convention on Narcotic Drugs of 1961, as amended by the 1972 Protocol; the Convention on Psychotropic Substances of 1971; and the UN Convention on Illicit Trafficking in Narcotic Drugs and Psychotropic Substances of 1988. In addition, the UNODC has established International Standards on Drug Use Prevention that provides a full set of measures to achieve a reduction in vulnerability and prevalence to drug use.

When specifically examining the prevention of tobacco use, studies have shown that high taxes are one of the most effective ways to reduce tobacco use, and in many regions illicit cigarette smuggling is more a response to weak regulation and law enforcement capability than to taxation. In addition, enhanced law enforcement capacity at local levels to identify and combat the illicit tobacco trade has also seen some success: in Bangladesh, effective on-ground enforcement over the last 5 years has reduced the share of illegal cigarettes in the market from 27% to 3%. Public-private partnerships to better control branding, quality control and supply chain integrity would also be of benefit to prevent cigarette counterfeiting, and diversion of stock onto the criminal market. Awareness campaigns about the health risks and associated harms may further reduce demand. The comprehensive means of addressing the illicit trade in cigarettes are laid out in the Framework Convention on Tobacco Control, which remains yet to enter into force due to an insufficient number of States Parties.

It is also important to note that in the area of over the counter medicines and illicit cigarettes, collaboration and engagement with the relevant private sector entities will be crucial. Managing the integrity of their supply chains, including enhancing security and monitoring at key transport notes and along specific transport, would greatly improve the integrity of products and brands. In the case of counterfeit medicines in particular, making essential life-saving medications available in greater quantities would reduce the market demand for illicit products. However, it is worthy of note that aid supplies of medication and pharmaceutical products are an established target for theft and resale by criminal groups, perpetuating criminal markets and threatening the viability of public health initiatives.

4 GOAL 14: Conserve and sustainably use the oceans, seas and marine resources for sustainable development

The global fishing industry plays an indispensable role as a supplier of essential nutrition, and is critical to food security in many vulnerable regions around the world. It is also one of the world's largest employers: the UN Food and Agriculture Organisation (FAO) estimates that nearly 180 million people are employed as fishers or in secondary industries relating to fishing activities. Consequently, conserving fish stocks and enforcing sustainable fishing practices are major contributing factors to achieving development goals. Yet, criminal practices in the fishing industry represent possibly the greatest threat to the conservation and sustainable use of the marine environment, and thus is a significant, if not the most significant, obstacle to achieving Goal 14.

In 2005, the FAO's 2005 Review of the World Marine Fishery Resources concluded that "75% of the world's fish stocks are fully exploited, overexploited, or depleted," which they attributed largely to the practice of illegal, unreported and unregulated (IUU) fishing. The practice depletes fish stocks; destroys natural habitats, leading to species becoming seriously threatened; reduces biodiversity, which in turn causes imbalances among species; and adversely affects ecosystems. Such imbalances and depletion, in addition to threatening Goal 14, may lead to a reduction of human food sources due to a scarcity of fish, hindering the achievement of Goal 2 (ending hunger and achieving food security).

Approximately 50% of fish exports are sourced from developing countries, which are most at risk from illegal fishing. IUU fishing undermines legitimate fishing competition, adversely affecting the livelihoods and economies in coastal communities, thereby impacting goals on poverty reduction, and makes fisherman more vulnerable to exploitation. Furthermore, the poaching of endangered marine life, such as abalone, has reduced stocks to endangered levels, which makes them more valuable as a commodity, thus intensifying the attraction for organised crime syndicates.

Moreover, the fishing industry has been extensively linked to other serious organised criminal activities, with human rights abuses and environmental crime often going hand in hand. The United Nations Inter-Agency Project on Human Trafficking suggests that trafficking into the long-haul fishing industry exemplifies the worst cases of labour exploitation. Incidents of crews including victims of trafficking is well documented. There is also evidence of widespread abuse of workers on fishing vessels, including accounts of seamen being thrown overboard and left to die.

5 GOAL 16: Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels

There is extensive evidence that confirms that the presence of organised crime significantly increases the insecurity and harm to civilian populations. Insecurity and injustice are a daily fact of life for a large proportion of people around the world, especially the poor. There is strong evidence and wide consensus that conflict and insecurity are major barriers to development. For example, all seven of the countries that are unlikely to meet a single Millennium Development Goal by 2015 are countries that have been affected by high levels of violence. Similarly, countries that experienced high levels of violence over the two decades between 1980 and 2000 were shown to have an average poverty rate 21% higher than countries with low levels of violence. Criminalised environments and political systems have given rise to extreme levels of armed violence, destabilised states and fuelled the armed activities of insurgent, radical and terrorist groups.

The United Nations has consistently emphasised the critical importance of strengthening and consolidating security and justice in the context of the rule of law, as being a pre-cursor and necessary condition for achieving stable and peaceful societies. Ever since the UN Secretary-General firmly asserted the "inextricable link" between security, human rights and development in 2004, the concept has now been well-entrenched in the rhetoric of international affairs. Early debates came in the context of post-conflict stabilisation and peacebuilding, and recognised the need to create "capable states" able to provide "security, well-being and justice," if vicious cycles of conflict, poverty and human vulnerability were to be brought to an end.

The attainment of good governance, sustained security and access to justice is fundamental for the rule of law, and is the basis of interstate relations and the fulfilment of international obligations. They are arguably the cornerstones of effective and sustainable conflict prevention and resolution, respect for basic human rights and fundamental freedoms, and the preservation and advancement of equal social and political rights, all of which serve as foundations of the principles of sustainable development. By contrast, crime, corruption and impunity threaten the legitimacy of the social contract, undermine the rule of law and slows, and perhaps even reverses, development progress.

Recent studies have shown how good governance and democratic processes have become very vulnerable to organised crime and corruption, particularly at the point of elections. This has impacts in the context of both developing and developed states. Infiltration into states and political processes has become a key goal for criminal groups, as globalisation has raised the stakes in terms of the potential benefits associated with criminal control over state re-

sources while simultaneously providing new means of ensuring impunity for both criminals and corrupt political actors. The increasing role, power and influence of money in securing electoral success have increased the vulnerability of political processes to criminal manipulation. Criminals are, of course, not meeting the compact of electoral office in providing social goods for the citizenship, nor are they substantially trying to influence the legislative process. Instead, the goal of criminal groups is to hollow out police and judicial institutions in order to facilitate their criminal enterprises. This is a situation with wide-ranging ramifications, not just for the legitimacy of democratic politics, but also for states' capacities to provide justice and the rule of law. To make matters even more challenging for development, the alignment of crime and politics further hinders women and marginalised groups, as they are less likely to be elected or stand for office in a context where there are high security concerns.

It has therefore become an increasingly frequent understanding of organised crime as a significant "external stressor" which undermines the capacity of key institutions and that leads to violence and conflict. Within that framework, increasing the measures to deter organised crime, arrest key criminal flows and criminal controllers, and buffer those most vulnerable from its impacts on development, governance, justice, security, human rights and the rule of law must be urgent priorities.

In recognising organised crime's impact on development, practitioners must work to understand and appreciate the pervasive and multi-faceted nature of the phenomenon. Organised crime manifests itself in a plethora of forms in theatres in nearly every corner of the globe. As such, organised crime cannot be viewed as a separate development obstacle to be addressed in isolation from other challenges and goals. Rather, an effective response calls for the recognition that organised crime is understood as an intrinsic element to nearly every development challenge, and must be interwoven throughout broader development response frameworks.

Moreover, by grouping different forms of organised crime together under single a target, the SDGs might not reflect the complexities of various forms of organised crime and illicit flows. For example, target 16.4 (By 2030 significantly reduce illicit financial and arms flows . . .) addresses illicit arms flows and illicit financial flows. While these illicit flows do overlap in a number of ways, the two are distinct criminal phenomena with differing root causes, actors, actions, flows, geographic foci, and impacts development, amongst other differences. In turn, to achieve target 16.4, practitioners will require an understanding and response to two different criminal threats, which can also take on very diverse forms in various regions of the world, and will certainly require a different set of responses to combat them.

Consequently, by isolating organised crime threats from other development goals and conglomerating various forms of criminal activities and flows under single targets, it is difficult to adequately explore the impact of organised crime on the goal and put forth sufficient and effective recommendations on modes of implementation.

Nonetheless, an attempt is made to fully capture the numerous obstacles organised crime poses to achieving Goal 16. Due to the diverse nature of organised criminal threats grouped under Goal 16, recommended responses are put forth under the relevant target, rather than clustered under the subcategory of Modes of Implementation, in an attempt to avoid confusion.

In the long term, a global strategy to counteract organized crime and corruption is needed, comprising a series of interlocking thematic and regional strategies. This will promote a more strategic, coordinated approach to counter organized crime and corruption by facilitating action at national, regional and international levels across a range of sectors and criminal markets. As this study demonstrates, the challenge is multi-faceted, with impacts across a range of domains – from humanitarian to developmental – yet there is currently no strategic platform that enables the kind of cross-sectoral, cross-regional debate and collaboration between the range of actors required to take forward a response.

5.1   Relevant targets under goal

– 16.1: Significantly reduce all forms of violence and related death rates everywhere

– 16.2: End abuse, exploitation, trafficking and all forms of violence and torture against children

– 16.4: By 2030 significantly reduce illicit financial and arms flows, strengthen recovery and return of stolen assets, and combat all forms of organised crime

– 16.5: Substantially reduce corruption and bribery in all its forms

– 16.6: Develop effective, accountable and transparent institutions at all levels

5.2 Modes of Implementation

As stated above, an enormous range of issues and challenges has been conflated in this goal, which makes it challenging to define a meaningful programme for its implementation. Moreover, the establishment of strong institutions takes decades of work by generations of politicians and officials, particularly in the cases of states emerging from conflict. Nevertheless, recognising that organised crime is a significant external stressor on communities' and states' capacity to achieve longer-term visions of governance, security and development is a good first step.

The Criminal Arboristic Perspective – A Method to combat Organised Crime

Kim Nilvall & Fredrik Mattsson

Swedish Police, Stockholm

The criminal arboristic perspective (CAP) is an analytical method that can be used to identify strategically important individuals within organised crime, to assess their capacity and prioritise the individuals towards which law enforcement measures should be aimed. The procedure increases the chances of predicting the direct or indirect effects any measures may have against strategically important persons.

Traditionally, organised crime is often described in terms of criminal networks or groupings. Our point of view differs from the traditional view in that we believe we should start from an individual perspective in order to understand and explain the structure of organised crime. The starting point for our reasoning is that the criminal world is no bigger than that all criminal individuals are linked to each other through the contact networks of the various individuals. Together they create a single large criminal network – organised crime.

In order to combat organised crime in a resource-efficient manner, we must identify individuals who are strategically important for the large criminal network. A simile with the work of an arborist can be made:

An arborist must know which branches can be pruned in order not to endanger the tree's supply of nutrients and water. The same applies conversely from a law enforcement perspective. Those individuals who have a strategically important role within organised crime are the branches that are particularly important to prune. If we only prune those branches that are the most easy to reach, we can cause the opposite effect – in fact, we are only strengthening organised crime by removing those parts that are weak so that they can be replaced by something stronger.

The analysis is based on an individual perspective and aims to assess the significance and duration of the relationships between individual criminals in the contact network. The contact network is divided up into two parts, an inner and an outer circle. The individual's inner circle consists of contacts that are more permanent, characterised by trust and frequent contacts over time.

The outer circle is more changeable, and may be characterised by limited trust and more sporadic contacts.

The objective of the work is in the first instance to bring the strategically important person to justice, or to disturb him, and in the second instance to bring persons in his inner circle to justice or to disturb them. It is also important to damage organised crime as a whole as much as possible. In order to use the resources as efficiently as possible, it is necessary to assess the capacity of strategically important criminals and prioritise between different targets. By using this model of assessing capacity and prioritising, the capacity of each criminal can be assessed – and therefore also the threat they pose to society.

The arboristic perspective and the method presented have several areas of application. For example, law enforcement authorities can use the method to identify "hidden" strategic individuals, to target informer recruitment onto the correct object, to lead and direct the operation on concrete and objective grounds, and for the purpose of follow up and evaluation.

Organised crime is often described in terms of criminal networks or groupings, but other concepts also exist. In Latin America, cartels are often spoken about, as are clans in the Balkans and families in Italy. The common factor for the designations is not that they reflect the actuality, but rather that they are based on how we have chosen to interpret and define organised crime, or how the criminals themselves have chosen to depict themselves. We consider that, as opposed to previous ways of looking at the issue, we must start from an individual perspective.

In sociology, a social network is described as a social structure made up from individuals linked together through one or several specific "links", such as friendship, kinship, common interests, and financial exchanges – relationships based on trust, knowledge or prestige. A social network can be described as a map of all relevant links between different individuals. A personal network analysis scrutinises and analyses the links or relationships between the individuals and make it possible to assess a person and his/her contacts and the joint capacity of the contact network.[1]

According to Stanley Milgram's hypothesis "six degrees of separation", all individuals on Earth are linked through at most five other individuals as intermediaries.[2] Research has also shown that persons, for example in a specific line of business or field of research, can be linked together through consider-

---

[1] Wellman, Barry & Berkowitz, S.D. (1988): *Social Structures: A Network Approach*. Cambridge: Cambridge University Press.

[2] Milgram, Stanley (1967): *The Small World Problem*. Psychology Today 2, pp. 60–67.

ably fewer steps, as they all belong to the same environment. This can be applied to the criminal world as well, as it can be regarded as a line of business.[3]

The criminal arboristic perspective (CAP) is a method for analysis that can be used to identify strategically important persons within organised crime, to assess their capacity and prioritise the individuals towards which law enforcement measures should be aimed. The procedure increases the chances of predicting the direct or indirect effects the measures may have against strategically important persons.

A simile between intelligence work and pruning a tree can be used to clarify this reasoning. If an arborist prunes a tree incorrectly, this may have consequences for the survival of the tree. An arborist must therefore know which branches can be pruned in order not to endanger the tree's supply system. The same applies from a law enforcement perspective –although the reverse – we must identify the persons within organised crime that constitute its life force. Those individuals who, from a law enforcement perspective, have a strategically important role within organised crime are the branches that are particularly important to prune. If we prune the branches that are the easiest to reach, it may have the opposite effect. We may then actually help organised crime by removing the weak branches, so that they can be replaced by new, stronger individuals.

A starting point when discussing criminal cooperation is to establish that every person has a social contact network, including family, relations, friends and colleagues, for example. Criminals also have various types of social contacts, of which some are maintained for criminal purposes. Just like law-abiding citizens, they turn to persons in their contact networks when they need help or services.

One example of this is how a criminal individual can use his contact network to get hold of a gun. The person in question contacts individuals in the own contact network, and if these cannot supply the need, they in turn contact other individuals in their respective contact network who may be able to sell a weapon. Via one or two "steps", the criminal may acquire in principle any article or service at all that is needed for the criminal activities. For a person outside the criminal sphere on the other hand, it is considerably more complicated to get hold of an illegal weapon.[4] The criminal world is no bigger than

---

[3] Morselli, Carlo (2009): *Inside Criminal Networks.* Springer.

[4] One example is when Sara Svensson, the nanny in the Swedish Knutby murder case, tried to get hold of a weapon. She had to travel in to Sergels Torg in central Stockholm and ask a large number of persons that she thought looked like criminals whether they could find a weapon for her. This clarifies her lack of a criminal contact network that could supply her specific need.

all criminals being able to intermingle with each other via a few persons. Together they create a single large criminal network – organised crime.

In order to illustrate the structure of a criminal's network, the persons that are part of it can be divided up into an inner and an outer circle. The individual's inner circle consists of contacts that are more permanent and is characterised by trust and frequent contacts over time. The outer circle is more changeable, and may be characterised by limited trust and more sporadic contacts. Persons included in the inner circle are the persons to which the individual has immediate access and together with whom he plans and/or carries out the criminal acts. The rest of the contact network – the outer circle – often includes persons who are used to carry out the riskier elements of a crime or who have specialist knowledge that is necessary for the crime. However, it should be emphasised that a person with whom an individual has committed a crime on one occasion is not automatically a member of the inner circle; instead other prerequisites are needed, such as having known each other over a long period.

The inner circle changes over time, and persons from the outer circle may become members of the inner circle at a later stage. The individual's contact network is therefore to be regarded as changeable rather than constant. It is also important to underline that relations that apparently are only social may partly also be – or may develop into being – criminal cooperation.

As both the inner and the outer circle are changeable, it is important to map the current contact network of individuals continually in order to identify possible perpetrators of future, current or past crimes.

In the event the strategic person has reached such a level within organised crime that it is difficult to bring the person in question to justice, the mapping of the individual's inner circle is central. It is within this circle that there are opportunities for interrupting and limiting the criminal actions of the strategic individual. In order to identify the person or persons within the inner circle against whom counteractive measures would be most successful, it is important to clarify each person's function in relation to the strategic individual, the benefit the strategic individual has of the person and whether the person has any specific skill or specific professional role.[5]

Once mapping of the inner circle has been carried out for several strategic individuals, it is probable that the strategic individuals have persons in common in their own respective inner circles. One example may be a person who

---

[5] These persons may fill a specific function in the crime, but rarely play any major part of the criminal operation as a whole (such as lawyers, accountants, money laundering experts, property brokers, bank officials).

supplied knowledge of money laundering and other advanced financial arrangements for a number of strategic individuals. This person can then also be regarded as strategically important, as the criminal activities of several other individuals within organised crime would be interrupted if the person was brought to justice.

In order to understand why certain persons carry out a crime together, knowledge about each person's contact network – and in particular the inner circle – is central. In order to clarify this reasoning, we can start from our own social networks and own inner circle. The inner circle consists of various types of contacts, such as family and close friends. For example, if we are going on holiday, we do not usually do so with the entirety of the inner circle, but with parts of it. The persons with whom we want to socialise are chosen depending on the activity to be carried out. On some occasions, persons from the outer circle are also included, such as acquaintances or colleagues from work. The persons who cooperate in a crime differ, depending on the character of the crime.

By applying the criminal arboristic perspective on organised crime:

Law enforcement authorities can better predict the effect of operational measures against an individual in an individual case and for organised crime as a whole. Thereby we can cause the greatest possible damage to organised crime in a resource-efficient way. By mapping the strategic individuals and their inner circles, we create the opportunity to assess and prioritise cases on a more clearly objective basis.

Law enforcement will gain a better understands how people are connected to each other and the meaning of the relationships. The method also makes it possible to make objective assessments in order to predict what effects crime prevention agencies actions might have.

If law enforcement know an individual's capacity through his inner circle of contacts we can also assess what over threat they pose together. If we prioritise on these bases we can also act strategically. We can also measure the success of the undertaken actions when we know which capacities we delimit for the targeted individual in the long run this means we act with a predicted effect.

Additionally, below is a brief summary of a number of different applications for the criminal arboristic perspective and how it can be used both operationally and strategically.

Primary fields of application

–   Identifying "hidden" strategic individuals

–   Creating a common structure for intelligence gathering and analysis

–   Capacity assessment of strategic individuals and their inner circles

–   Quicker identification of unknown persons during covert telephone interception, covert telephone surveillance and covert room surveillance

–   Tools for identifying possible collaborators in planned or past crimes

Informer handling

–   Strategic recruitment

–   Evaluation of source information

–   Assessing the informer's access to information

Management and direction of the operation

–   Objective basis for prioritisation and decisions

–   Linking strategic direction with operational work

–   Possibility of predicting the effects a measure against an individual may have in a specific case and for organised crime as a whole

Follow-up

–   Structured reporting

–   Evaluation of effect in relation to input

Fighting Organised Crime with Technology in Poland – the Results of Research Projects

Wojciech Filipkowski[1]

University of Bialystok, Faculty of Law, Poland

The studies the author has been involved concern the acquisition and the use of technology by law enforcement agencies, special security services, and criminal justice for the needs of operational or criminal procedures conducted by them for detection or evidence purposes, as appropriate. Unlike the traditional approach to the issue, the research focused on the use of the most recent technological solutions in this area, mostly pertaining to information technology. Criminalistic tactics also include the rules for purposeful and effective use of technical means in the fight against crime. This was another aspect of the research. The thesis was proposed that the achievements of contemporary information technology in the area of acquisition and analysis of information can contribute to a more effective fight against crime, including organised crime. Moreover, it was emphasized that the solutions adapted most rapidly are those intended to prevent and combat the most serious categories of crime, in particular organised crime and terrorism. This is due to the fact that the solutions sought are those that improve the effectiveness of the operation of state bodies in dealing with such crimes, which are hard to detect and persecute in traditional ways.

Information technology solutions are appreciated by practitioners but are overlooked by the science of criminalistics. This issue has become the subject of the session of Committee II entitled "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime" during the 12th United Nations Congress on Crime Prevention and Criminal Justice held in 2010 in Salvador, Brazil (Pływaczewski, 2010: 133 and ff).

---

[1] E-mail: w.filipkowski@uwb.edu.pl; URL: http://www.prawo.uwb.edu.pl.

The author has conducted researches in the following fields:

– Contemporary technologies supporting law-enforcement agencies, security services, and criminal justice in the fight against organised crime.

– Evaluation of usefulness of evidence obtained by using technological solutions at the stage of operational-reconnaissance activities, with particular focus on criminal intelligence analysis.

– The most recent information technology solutions that can improve the effectiveness of actions undertaken by law enforcement agencies, security services, and criminal justice.

– Research on the criminalistic aspect of criminal intelligence analysis.

1 Contemporary technologies supporting law-enforcement agencies, special services, and criminal justice in the fight against organised crime

In the initial stage the author's interests in this relatively new field of criminalistics were realized in the framework of the tailored research project commissioned by the Ministry of Science and Higher Education entitled "*Monitoring, identification, and countering threats to citizens' security*" managed by Professor Emil W. Pływaczewski (Filipkowski, 2012: 107–122). This was also due to the author's involvement in the works of the Polish Platform for Homeland Security (Pływaczewski, Guzik-Makaruk, 2015: 219 and ff) association where practitioners of law enforcement and criminal justice as well as scholars – from the humanities and engineering strive to develop technologies for state agencies intended to ensure security and public order.

As a part of the project, upon the initiative of the author's criminalistic research, the first of this type in Poland was conducted on contemporary technologies used by state agencies in the fight against organised crime. Part of the research consisted in selecting three groups of respondents. It was assumed that the group with the most extensive knowledge on the use and suitability of technologies in the fight against organised crime is persons who are involved in this effort on a daily basis. Such a group comprises officers of the Central Bureau of Investigation of the National Police Headquarters (Filipkowski, 2010a: 71–89)[2], public prosecutors from appellate regional public

---

[2] The research material, comprising 245 surveys, was obtained; all in all, 77% of all the respondents who have received the surveys filled them out and returned them.

prosecutor's offices (Filipkowski, Pogorzelski, 2012: 135–151)[3], and judges of criminal divisions of appellate courts (Filipkowski, 2010c: 253–273)[4].

The study aimed at collecting the opinions of selected groups of respondents concerning their contacts with new technologies in their work connected with fighting organised crime. The objectives of the research were to collect the respondents' opinions about the presence of such technologies in their work, to determine how the existing solutions can be improved, and to indicate solutions that are the most desired and useful in their work.

1.1   Contemporary technologies

Based on their professional experiences, the respondents were asked to indicate, the technological support they have obtained in their work related to the fight against organised crime. The list was elaborated based on information received during informal interviews conducted with practitioners working in law enforcement and criminal justice. The first group comprised technologies known in criminalistics, namely[5]:

– localization of persons (using GPS and BTS technology);

– criminal intelligence analysis of financial and personal ties;

– analysis of the history of bank accounts and financial transactions; and

– access to computerized databases with information on persons, events, and objects (hereinafter referred to as computerized databases).

---

[3] The research covered 55 surveys from appellate public prosecutor's offices and 299 surveys from regional public prosecutor's offices. It is estimated that at the time the research was conducted, the entire population of the first group of respondents was about 126 persons and of the second group – approximately 652 persons. Thus, the research covered 44% of public prosecutors in the first group and 46% of public prosecutors in the second group.

[4] The total number of the surveys filled out and returned by the respondents from all the appellate courts in Poland was 45. Thus, the survey covered one third of the entire population. At the time of the research, approximately 135 judges worked in criminal divisions of appellate courts.

[5] The respondents were also able to add and to evaluate other types of technological support not included in the list they were presented them. However, they took advantage of this possibility only rarely.

The second group included two kinds of technology supporting the work of law enforcement agencies in purely technical aspects:

– remote interrogation of witnesses (via teleconference); and

– sending electronically information included in criminal cases.

It was visible that significant differences between groups of respondents with regards to contacts with new technologies in their work connected with the fight against organised crime. It is worth noting that it was public prosecutors were those who the most extensive contacts with new technologies, regardless of their type. The judges were on the other extreme. Of course, this was due to the unique characteristics of the work of each of the respondent groups. It appears that the result of the study involving the prosecutors group was connected with the fact that they used the products obtained by using new technologies at the stage of operational-reconnaissance activities conducted by law enforcement agencies and had their own technical tools, such as computerized databases and analyses prepared by analysts working at public prosecutor's offices.

There were also differences in the types of technological support useful in their work. Therefore, there is little wonder that teleconferences were not as commonly mentioned by police officers as they were by judges. What is surprising is the lowest rank of this technology in the opinion of public prosecutors. On the other extreme, there were technologies allowing locating persons, criminal intelligence analysis, and access to databases, which were familiar to a much larger percentage of respondents in the police officers group than in the judges group. This was also connected with their scopes of duties.

The technologies listed were mostly connected with the preparatory proceedings stage or even the operational activities; therefore, compared to the other, a much smaller percentage of respondents in the group of judges, declared that they had encountered such technical solutions. They reported most frequently using criminal intelligence analysis pertaining to records of financial transactions (nearly 65% of the respondents), followed by localization of persons and criminal intelligence analysis pertaining to financial and personal ties (approximately 50% of the respondents). Only the third in the ranking was the technology that could be used by judges themselves, namely remote interrogation (over 40%). The respondents most often encountered access to computerized databases containing information on persons, objects, and events.

1.2   Proposals concerning technological solutions

The respondents were asked to identify technologies that were not enumerated in the questions they were asked concerning proceedings in organised crime cases. This question was an opportunity for the respondents to point out shortcomings in the current legal system and the limitations in access to technologies. Unfortunately, only a few respondents in each of the research groups took advantage of this opportunity. This could have been due to their positive opinions about the current level of saturation with technologies intended to support the fight against organised crime, to a lack of clear and precise opinions in this area, or to the respondents' unwillingness to answer open-ended questions[6].

In the police officers group, only 33 of the 245 respondents provided an answer to the open-ended question. The answers given can be divided into the following groups:

1. difficult access and functioning of the existing computerized databases;

2. low level of technological advancement of the equipment used by the police;

3. difficult cooperation with mobile communication network operators.

The same question was answered by only 57 public prosecutors of appellate and regional public prosecutor's offices. Respondents from appellate public prosecutor's offices indicated, among others, the need to broaden and speed up (by making it less formal) the access of prosecutors to existing databases, to include those operated by the police, to establish additional databases and with the prosecutors having direct access to them, to create a system that would enable automatic transcription of speech, and to make analysis programs related to criminal proceedings operated by various institutions uniform so as to facilitate flawless transferring and processing of data.

The respondents from regional public prosecutor's offices also indicated the need to expand access to databases. They also emphasized the need to increase the number of certified workstations and wiretapping equipment, to provide internet access to public prosecutors, to increase the number of specialists and analysts in order to operate special criminal intelligence analysis

---

[6] Of the entire group of 45 respondents in the group of judges from criminal divisions of appellate courts, only 4 answered this question.

software, to equip public prosecutor's offices with equipment and software enabling properly securing information technology data in criminal proceedings so as to avoid the need to assign experts.

1.3   Anticipated directions of research and development

The survey was also an opportunity for potential future users of new technological solutions to discuss the subjects of scientific research in the area of technology and to evaluate their usefulness in the fight against organised crime. The respondents were asked to rank several technological solutions presented to them, based on their professional experience, from the most to the least needed in cases involving organised crime.

It must be noted that a part of the technical solutions presented in the question were mentioned by some respondents as ways to solve the problems they encountered in their professional work. None of the solutions was found by any of the respondent group as the most or least needed. The subjective approach of the respondents to the technological solutions is not surprising. The solutions that were the most needed were those that could directly facilitate their work.

The results were similar throughout the groups. The differences were due to the professional experiences of the different groups of respondents. In the case of police officers and public prosecutors, the respondents indicated that the most solutions needed were tools for automated criminal intelligence analysis (based, among others, on artificial intelligence), which would cover telephone records (billings or traffic data), financial transactions, and relationships within criminal groups. The judges, on the other hand, mentioned the so-called "electronic files" intended to be used in criminal proceedings. This does not raise any concern as the respondents directly encountered files in criminal cases, which are still in the paper form. This solution would facilitate their work and, consequently, is the one most needed, according to the respondents. The participating police officers and public prosecutors ranked this solution behind criminal intelligence analysis.

The postulates made by all respondents concerning automation of the process of performance of criminal intelligence analysis are not surprising, given the number of persons and events that need to be analysed during proceedings involving organised crime. Implementation of this solution can significantly facilitate determination of directions of specific preparatory proceedings and speed up the achievement of their objectives.

According to the respondents, solutions intended to provide purely technical support to government bodies were the least needed. Automatic transcription of speech could bring a revolutionary change in the preparation of reports from interrogations or court hearings. In this case, too, the respondents declared that these instruments were more needed than other technologies. According to the respondents, the least needed technological solutions, were tools for automatic translation of speech from foreign languages into Polish and tools for deciphering communication between criminals.

1.4   Conclusions

In addition to the detailed conclusions presented above, the following general propositions concerning the methods of research on the technological solutions to be used by government bodies responsible for ensuring security and public order and for administration justice were formulated:

At the stage of designing of solutions it is necessary to involve future end users, in order to ensure the prototypes match the needs of the users to the maximum extent possible.

Lawyers should be actively involved in the works of the teams designing the technological solutions for use in the area of security and administration of justice. Their tasks should include making the engineers aware of the existing legal constraints and proposing changes in the current laws in order to enable using the most effective technological solutions.

The engineers who in their work do not take into account the legal aspects of the problems faced by law enforcement agencies and the judiciary can discover new and potentially more effective ways to solve those problems.

Representatives of law enforcement agencies and the judiciary should be concerned about new technological solutions that can accelerate and make the performance of numerous tasks more efficient. Their criticism should be constructive and free from personal prejudices, habits, and fears of new technologies.

Financial constraints can be overcome by using funds available in Poland (e.g. from the National Research and Development Center) and abroad (in particular on the level of the European Union), as well as by forming public-private partnership or by commercialization of the scientific research.

2 Evaluation of usefulness of evidence obtained by using technological solutions at the stage of operational-reconnaissance activities, with particular focus on criminal intelligence analysis

The same respondent groups in the second part of the prepared research tool were asked to express their opinion about the legal and organisational instruments in the system of prevention and suppression of organised crime[7]. Only the results of this part of the research will be presented as the respondents provided their opinions concerning the use of, among others, results of criminal intelligence analysis as evidence.

The first question in this section of the survey concerned evaluation of the frequency of use and usefulness of the evidence obtained by way of operational-reconnaissance activities. The following list was presented: wiretapping, personal sources of information (informers), covert recording of video material, covert monitoring of movement of persons, room tapping, electronic correspondence control, mail control, criminal intelligence analysis, and controlled handing of financial benefits (bribes).

Officers of the Central Bureau of Investigation of the National Police Headquarters concluded that of the 9 items, only evidence from personal sources of information, wiretaps, and covert monitoring of movement of persons were more useful than evidence obtained as a result of criminal intelligence analysis at the stage of operational-reconnaissance activities. In this group, only the evidence from personal sources of information (informers) was used more often than the evidence obtained by way of criminal intelligence analysis (Filipkowski, 2009: 136–164).

The same question was asked of a group of public prosecutors from appellate and regional public prosecutor's offices (Filipkowski, Pogorzelski, 2011: 89–109). In the case of the respondents from the former group, most opinions about evidence from wiretaps, personal sources of information (informers), and criminal intelligence analysis were positive. The results obtained in the latter group were similar. The respondents from regional public prosecutor's offices had higher opinions of evidence obtained by way of criminal intelligence analysis than of evidence obtained from personal information sources (informers). Such evidence was used more often during preparatory proceedings in cases involving organised crime than in other operational-reconnaissance activities.

---

[7] Because none of the surveyed judges had encountered in his or her professional work results of criminal intelligence analysis, they did not evaluate the suitability of evidence obtained by using this tool (Filipkowski, 2010b: 157–172).

3 The most recent information technology solutions that can improve the effectiveness of actions undertaken by law enforcement agencies, security services, and criminal justice

3.1 Analysis of financial transactions

Contemporary technological solutions can be used successfully in the area of security and public order. Experts from both fields of knowledge need to cooperate in this area. This is true in the case of identifying of suspicious transactions involved in money laundering and financing of terrorism, as well as in fraud (Dreżewski, Filipkowski, Sepielak, 2009: 81–102; Dreżewski, Filipkowski, Sepielak, 2012: 8–21)[8].

The growing demand on the part of law enforcement administration and the judiciary for information technology tools for processing bulk quantities of data has been the basis for research on criminalistic and process-related aspects of the use of such tools. In particular, these include technologies based on artificial intelligence, and machine learning. To a large extent these tools can take the place of people in schematic, repeated activities performed in accordance with specific algorithms. Machines can make conclusions based on the data entered into them or by using expert knowledge in their algorithms which, given their higher computational capacity, compared to people, may turn out to be an effective tool for analysing bulk quantities of data. This is why the concept of evidence from academic research should be discussed. The scholars working to expand this field of knowledge need to refine and elaborate procedures and methods of criminal intelligence analysis in a way that will enable using the effect of their work as evidence in criminal cases.

It must be emphasized that data mining, as a part of the concept of knowledge discovery in databases, has become the most important among the analysed technologies (Seifert, 2008; Pal, 2011: 8). This is demonstrated by a number of examples of its use in criminalistics abroad, for instance for the purpose of:

– performing criminal intelligence analysis (both operational and strategic);

– profiling of perpetrators;

---

8   The author's recommendations have been implemented as a plug-in of the LINK platform (called The Money Laundering Detection System) developed by a research team from the AGH University of Science and Technology. This is a criminal intelligence analysis tool that can be used successfully to detect such money laundering techniques as distribution and collection accounts, structuring, and quick deposit & withdrawal. The platform uses search algorithms, the so-called sequence miner used in data mining.

–   identifying dangerous persons (potential assassins and terrorists);

–   identifying suspicious transactions;

–   supporting the process of dislocation of patrols;

–   search for attempted attacks against critical infrastructure through the internet;

–   detecting anomalies in the behaviour of persons; and

–   analysing links between persons in social media.

Data mining enables identifying certain, frequently unexpected or unknown, patterns and relationships within specific sets of data by performing various manipulations of the data, e.g. by structuring, classification, regression, etc. Legal and criminalistic research is important as the use of data mining involves the need to solve a number of legal and criminalistic problems, to include those related to restrictions in laws on personal data protection and to methods of use of data mining in preparation of criminalistic analyses. The problem of data mining use by law enforcement agencies, security services, and the judiciary in criminal intelligence analyses has become one of the research areas included in the current development project managed by Prof. Emil W. Pływaczewski entitled "Modern technologies for and in the criminal process and their use – technical, criminalistic, criminological, and legal aspects." (Pływaczewski, 2014: XV–XVI).

3.2   Further directions of joint research of penal sciences and technological sciences

The author has also conducted research on the directions that must be taken in order to develop legal and technological solutions intended to enhance security and public order, including the fight against organised crime (Filipkowski, 2011: 261–275). It was pointed that there is a need to conduct research in the following areas:

The law remains the most important tool of the state in the area of regulating individual's and group's behaviour. The only question is the extent of such regulation. Dogmatic research must to be done regarding the need for and the way of regulating social phenomena, about changes in the society, various pathologies, and about technological progress.

Multi-level, comprehensive research on the social phenomena mentioned above. The products of cooperation and the synergies achieved thanks to the efforts of scientists and practitioners from various humanities and technical fields must be used to solve social problems.

Research on public-private partnerships aimed at ensuring security. Reduction of the powers of state bodies responsible for ensuring public order and security or reduction of their funding and staff leads to private entities naturally filling the void. It is necessary to define the scope of their powers and relations with state bodies, local authorities, etc. This includes the issue of commercialization of the results of scientific research in the area of security.

Better use of generally accessible information (its acquisition, gathering, evaluation, and use), in particular information found on the internet and in social media (e.g. monitoring and forecasting of events based on entries in social media).

Integration of databases and information technology systems of different state bodies and shared systems in order to reduce their operating costs and enhance the cooperation among various state bodies.

Enhancement of interoperability of different information technology solutions offered by various providers to state bodies, for instance by normalizing the information exchange protocols, automating acquisition, analysis, and use of information contained in private and government databases.

4 Research on criminal intelligence analysis in the criminalistic aspect

4.1 Introductory problems

From the long list of technical instruments used in the fight against crime, it was criminal intelligence analysis that was selected as the subject of the latest research (Chlebowicz, Filipkowski, 2011)[9]. It constitutes practical implementation of solutions that are often based on advanced and quickly developing fields of computer science such as artificial intelligence, neuron networks, and knowledge discovery in databases. In addition, in respect to the opera-

---

[9] The research was conducted in the framework of the research and development project of the Ministry of Science and Higher Education entitled "Legal and criminological aspects of implementation and use of modern technologies intended for strengthening internal security" (Płaczewski and others, 2010: 199–201) from 2009 to 2011 on which the author was the Project Manager.

tional and strategic aspects, criminal intelligence analysis is the embodiment of the idea of intelligence-led policing where law enforcement and public order bodies perform their operations based on knowledge (Carter, Carter, 2009:310–325; Ratcliffe, 2003: 1–6). This idea has resulted in the formation of a completely new field of knowledge that is, within criminalistics, referred to as criminal intelligence[10].

The object of the research was criminal intelligence analysis as an activity performed in the practice of law enforcement agencies and the judiciary. It was found that criminal intelligence analysis is a phenomenon of dual nature. It is used both as a part of operational-reconnaissance activities and during criminal proceedings. The technical aspects of its use are similar regardless of the types of activities performed. The law only provides for different ranges of data that can be used in it depending on whether it is performed before or during a criminal process.

Due to a limited access to theoretical studies of criminal intelligence analysis, it was necessary to conduct empirical research on this subject. The research focused on the practical use of criminal intelligence analysis by Polish state bodies. Taking into account the scope of the research questions, it was necessary to precisely define the populations to be studied. It was found that the persons who have the most extensive knowledge and experience in the performance of criminal intelligence analysis are those who perform it as a part of their duties. The study was performed by gathering the opinions of criminal intelligence analysts working in law enforcement agencies, security services, and public prosecutor's offices[11].

---

[10] It must be emphasized that the research area studied by the author so far has not been the object of in-depth analysis in Poland. Since the mid-1990s there have been only several papers describing the capacity of criminal intelligence analysis in the Polish literature (Kobylas, 2015: 96 and ff).

[11] The text of the survey was consulted by representatives of law enforcement agencies and the judiciary who are familiar with the problem of criminal intelligence analysis. During the research, the appropriate official permits for the research was obtained. The principal part of the research was conducted in the 4th quarter of 2009 and the first half of 2010. It was assumed that the survey forms were filled out by all or nearly all respondents in the assumed professional groups. All in all, the population covered by the research can be defined based on the number of surveys filled out in the respective institutions: Police – 83 surveys, Border Guard – 35 surveys, Central Anti-Corruption Bureau – 17 surveys, and Public Prosecutor's Office – 95 surveys.

4.2 The research results

The proposed typology of criminal intelligence analysis according to the type of information has demonstrated that the practical implementation of this type of analysis differed.

In each of the professional groups covered by the study, analyses of telephone records (billing or traffic data) were most often used. Such data contains a fairly large amount of information that can be used to conduct analyses and to make more extensive determinations than who contacted whom. Examples include social networks analysis, description of habits and routine behaviour, and change of location by phone users, etc. On the other hand, the use of different types of analyses also depended on the experience of the analysts, the scope of responsibilities of the professional group, and legal restrictions on the access to data that could be analysed.

The criminal intelligence analysts mostly used two types of software: spreadsheets and data visualization software. The latter could not be used without prior preliminary processing of the data in a spreadsheet. This fact has not been properly appreciated in the literature on the criminal intelligence analysis. This also indicated the scope of knowledge and skills required of criminal intelligence analysts.

The criminal intelligence analysts worked mostly on data contained in telephone records and financial transaction records. The data contained a great deal of additional information that could be used in further, more advanced analyses using, for example, social network analysis or data mining methods. In the case of the latter, the more data is available for analysis, the better (more precise and reliable) are the results of that technique. What is also important is the fact that in most cases the data is already in the digital form.

Regardless of the professional group they belonged to, the most desirable software mentioned by the respondents was the one which allows the visualization of routes travelled by mobile communication users. Thus, the importance of data found in telephone records was confirmed one more time. The second group of expectations concerned solutions that would make their work easier through automation and acceleration of analyses. Only the third in the order of importance was access to various databases, such as government and ministerial databases, and databases of other law enforcement agencies. What was surprising was that the fact that analysts' use of information found in social media portals (like Facebook) was confirmed.

The respondents emphasized, directly or indirectly, that the general objective of criminal intelligence analysis is to systematize and visualize the data defined in their work assignment. The analysts emphasized that quite often the objectives of analyses depended on the needs of the entity who ordered the

analyses for their operational-reconnaissance activities or criminal proceedings activities. This clearly depended on the entity's level of knowledge of the various options associated with different types of data.

In the opinion of the respondents, the quality and completeness of data contained in telephone records and of the data needed to perform an analysis of personal ties or events were good or average. It appears that the heterogeneity of the sources led to better opinions of the completeness and quality of the data. Missing or incomplete data from one source could be supplemented or confronted with data coming from another source.

In general, the respondents found criminal intelligence analysis to be useful at each of the stages, to include in preparatory proceedings and court proceedings. However, the largest number of respondents by far, regardless of the type of analysis and professional group, declared that criminal intelligence analysis is the most useful during operational-reconnaissance activities.

In the opinion of the respondents, the problem that occurs while conducting criminal intelligence analysis is access to larger quantities of data in an electronic form. In the case of data provided by telephone operators and financial institutions, the fundamental problem mentioned by the respondents was lack of uniform standards in the way the data is being gathered and recorded. This leads to the need to manually process the data provided by various institutions to achieve a uniform format using spreadsheets which takes a lot of time. Only then could such data be imported into the visualization software. In addition, the data contained erroneous entries, was incomplete, or described in an incomprehensible manner. On the other hand, in the case of data needed to perform analyses of personal ties and events, the problems reported by the respondents were as follow: the quality and credibility of data entered by multiple entities, access to databases, and the fact that the knowledge contained in the data is scattered.

4.3   Postulates resulting from the research conducted

The results of the research enabled formulating the following postulates:

– The contemporary form of criminal intelligence analysis is a new area in the 21st century science of criminalistics. There is no doubt that the great capabilities of information technology tools will soon enable performing criminal intelligence analyses using artificial intelligence methods.

– New research areas should be indicated; this includes problems related to elaboration of a uniform method of performance of criminal intelligence analyses as well as criteria and requirements for persons performing criminal intelligence analyses.

– Criminal intelligence analysis should be mandatory in complicated and multi-threaded cases especially regarding organised crime and terrorism.

– Simple analytical techniques, based on basic software, should be propagated among the so-called "first line" officers. This way, highly-qualified criminal intelligence analysts should be involved only in the most difficult cases, including ones connected with organised crime and terrorists activities.

– With reference to the aforementioned capabilities, not only operational-level but also strategic-level criminal intelligence analysis should be developed in Poland.

– The objectives of criminal intelligence analysis are in line with the objectives defined in both the Polish Code of Criminal Procedure of 1997 and the Police Act of 1990. Unfortunately, due to the development of new technologies, there are areas of potential abuse of the powers which may take the form of excessive or disproportional surveillance.

Bibliography

Carter, D. L. and Carter, J. G. (2009), Intelligence-Led Policing. Conceptual and Functional Considerations for Public Policy. Criminal Justice Policy Review, No. 20(3), 310–325.

Chlebowicz, P. and Filipkowski, W. (2011), Analiza kryminalna. Aspekty kryminalistyczne i prawnodowodowe [Criminal intelligence analysis. Criminalistic and law of evidence aspects]. Warsaw: Wolters Kluwer.

Dreżewski, R., Filipkowski, W. and Sepielak, J. (2009), Analiza przepływów finansowych [Analysis of financial transactions]. in: E. Nawarecki, G. Dobrowolski, M. Kisiel-Dorohinicki, eds., Metody sztucznej inteligencji w działaniach na rzecz bezpieczeństwa [Artificial intelligence methods in actions aimed to improve security]. Kraków: AGH, Kraków, 81–102.

Dreżewski, R., Filipkowski, W. and Sepielak, J. (2012), System supporting money laundering detection, Digital Investigation, Volume 9, Issue 1, 8–21.

Filipkowski, W. (2009), Prawne i organizacyjne instrumenty zwalczania przestępczości zorganizowanej w opinii funkcjonariuszy Centralnego Biura Śledczego [Legal and organizational instruments for fighting organized crime in the opinion of officers of the Central Bureau of Investigation]. Białostockie Studia Prawnicze, book 6, 136–164.

Filipkowski, W. (2010a), Rozwiązania technologiczne w pracy policji na podstawie badań ankietowych [Technological solutions in the work of the police based on survey research]. Przegląd Policyjny, No. 1, 71–89.

Filipkowski, W. (2010b), Ocena wybranych instytucji służących zwalczaniu przestępczości zorganizowanej [Evaluation of selected institutions charged with combating organized crime]. Ruch Prawniczy, Ekonomiczny i Socjologiczny, book 2, 157–172.

Filipkowski, W. (2010c), Technologiczne aspekty walki z przestępczością zorganizowaną" [Technological aspects of combating organized crime]. in: J. Kasprzak, B. Młodziejowski, eds., Wybrane problemy procesu karnego i kryminalistyki [Selected problems of criminal process and criminalistics]. Olsztyn: Warmia i Mazury University in Olsztyn, Faculty of Law and Administration, 253–273.

Filipkowski, W. (2011), Nowe kierunki badań nad bezpieczeństwem w Polsce i ich efekty [New directions of research on security in Poland and their effects]. Białostockie Studia Prawnicze, No. 9, 261–275.

Filipkowski, W. (2012), Wybrane aspekty technologiczne walki z przestępczością zorganizowaną [Selected technological aspects of the fight against organized crime]. Przegląd Policyjny, No. 1, 107–122.

Filipkowski, W. and Pogorzelski, J. (2011), Legal instruments intended for the fight against organized crime in the opinion of public prosecutors. in: W. Pływaczewski, ed., Organized Crime and Terrorism. Reasons – Manifestations – Counteractions. Olsztyn: University of Warmia and Mazury, 89–109.

Filipkowski, W. and Pogorzelski, J. (2012), Technological aspects of the fight against organized crime in the opinion of public prosecutors. in: E. W. Pływaczewski, ed., Current Problems of the Penal Law and Criminology, Warsaw: LEX a Wolters Kluwer business, 135–151.

Kobylas, M. (2015), Wykorzsyatnie analizy kryminalnej w zarządzaniu informacja w Policji [The use of criminal intelligence analysis in managing information in Police], in: E. W. Pływaczewski, W. Filipkowski, Z. Rau, eds., Przestępczość w XXI wieku. Zapobieganie i zwalczanie. Problemy technologiczno-informatyczne [The Criminality in XXI Century. Prevention and Combating. Technological and Informatics Problems], Warszawa: Wolters Kluwer, 91–107.Pal, J. K. (2011), Usefulness and application of data mining in extracting information from different perspectives, Annals of Library and Information Studies, No. 58, 7–16.

Pływaczewski, E. W. (2010), Zapobieganie przestępczości i sprawiedliwość karna: XII Kongres Organizacji Narodów Zjednoczonych (Salvador, Brazylia, 12-19 IV 2010) [Preventing crime and criminal justice. The XII United Nations Congress (Salvador, Barsil, 12th-19th of April, 2010]. Państwo i Prawo, No. 10, 133–135.

Pływaczewski, E. W. and Guzik-Makaruk, E. M. (2015), Polish Platform for Homeland Security and its place in the research on security in Poland. in: J. Dworzecki, ed., Selected aspects of internal security. New York: Inglobal Writer Inc., 219–234.

Pływaczewski, E. W., Laskowska, K., Szczygieł, G. B., Filipkowski, W., Guzik-Makaruk, E. M. and Zatyka, E. (2010), Polskie kierunki badań kryminologicznych nad bezpieczeństwem obywateli [The Directions of Polish Criminological Research on Citizens' Security]. Prokuratura i Prawo, No. 1–2, 176–200.

Pływaczewski, E. W. (2014), "Current Problems of the Penal Law and Criminology" in retrospect and from a contemporary standpoint. in: E. W. Pływaczewski, ed., Curent Problems of the Penal Law nad Criminology. Warszawa: C. H. Beck, XI–XXI.

Ratcliffe, J. (2003), Intelligence-led policing. Trends & Issues in Crime and Criminal Justice, No. 248, 1–6.

Seifert, J. W. (2008), Data Mining and Homeland Security: An Overview, Updated April 3, 2008, CRS Report for Congress, Order Code RL31798.

Trafficking in Humans in Hungary –
Perpetrators, Victims, Prevention and Prosecution

Szilveszter Póczik

National Institute of Criminology, Budapest, Hungary

A Roma family bought a young woman for an amount of 5,000 HUF (16 euro) and treated her as a slave for a period of 8 years, forcing her to prostitute herself. She was not the only person having been prostituted by the same family for a long time. In the course of their arrest, another young woman who has been forced to slavery and street prostitution for 8 years was also freed. She was accommodated in a shed behind the residential house and beaten several times.[1]

Spot 46, a centre for information and advice for sex workers in The Hague is an NGO that runs shelters for runaway prostitutes, protects them against the traffickers, hires advocates for the protégées as well as offers financial aid to them that they learn the country's language and find an ordinary job. It is unknown how many foreign prostitutes are living in the Netherlands because prostitutes are not obliged to register themselves, making only estimations are available. According to Maaike van Groenestyn, project leader of Spot 46, their number is around 25,000 to 30,000. The most of them are Hungarians, Rumanians, Bulgarians and those from Central-America. About the half of the prostitutes working in The Hague and one third in Amsterdam are Hungarians. It is particularly difficult to contact them because the well organised professional trafficking networks and local pimps from Hungary are very aggressive. Not only the women but also the social workers who are trying to help them are intimidated.[2] The majority of Hungarian prostitutes are of Roma origin without any professional qualification from Roma slum neighbourhoods and poor small villages of North-Eastern Hungary in an age of 18–25 years but there are some juveniles – e.g. escaped from an orphanage or

---

[1] *Buzna*, Viktor: Pénzen vett lányok kálváriája [Calvary of girls bought by money]. Magyar Nemzet, May 26, 2015, http://mno.hu/magyar_nemzet_belfoldi_hirei/penzen-vett-lanyok-kalvariaja-1287864.

[2] *Bérczes*, Tibor: Hollandia legborzasztóbb utcája - Maaike van Groenestyn a magyar prostituáltakról [The most terrible street in the Netherlands - Maaike van Groenestyn reports on Hungarian prostitutes]. Magyar Narancs No. 24, 2012 (June 14), http://magyarnarancs.hu/szex/hollandia-legborzasztobb-utcaja-80468.

a closed education institution – with false ID-documents, too.[3] The most of them were forced to work as prostitutes in Hungary before coming to Holland. In many cases they were sold by their families to the traffickers who brought them abroad. The girls know only that they are in The Hague or Amsterdam but are only allowed to attend the grocer nearby. They are world-weary, indifferent, depressed, being under alcohol and/or drug influence, without language knowledge and social contacts. Their knowledge in their mother tongue is very poor, too, many are illiterate. Many of them have own children under the care of the grandparents and the pimps press these girls, saying "you will never see your baby again".

The "Hungarian prostitute" became – based of her status and services – a separate category being on the lowest level of the red light scene. The Hungarian prostitutes are extraordinarily slovenly and scruffy, even more than those from Romania or Bulgaria. Despite this, they are popular amongst the clients as a number of the girls do not use condoms – partly because they do not understand the importance, partly because the pimps forbid it in order to claim a higher price from the clients who are even allowed to humiliate, beat or torment the girls. The johns do not need to be afraid of getting denunciated to the Police. The Hungarians are working in the small street Molensteeg that received the nickname "Nyiregyháza" after an East-Hungarian town.[4] They are the cheapest on the market and that is why mostly hated by other prostitutes. They are literally slaves of the traffickers. In average 50 percent of the traffickers' victims turn to the police, but Hungarians almost never do. They are misused and mishandled by the pimps daily, and forced to hand over all their earnings.[5]

The situation in Zurich is quite similar. The street prostitution is banned into the periphery District 19, not far away from the elite red light areal of sex bars, hotels and brothels. At the end of a one-way-street roofed parking places, so-called sex boxes are built for clients where they make use of the services of the prostitutes in their cars. The social background of the Hungarian girls is the same as in Amsterdam[6]: lower class, poverty, extraordinarily

---

3   *Tamási*, Erzsébet: Budapest – Prostitúció. A fővárosi prostitúció rendészeti szempontú vizsgálata [Budapest – Prostitution – Research of Street prostitution in the Capital from Police point of view]. National Institute of Criminology - OKRI, Budapest, 2015. p. 105.

4   To the situation of street sex workers in the real existing town Nyíregyháza see the website of Periféria Egyesület /Periphery Association: http://www.periferiaegyesulet.hu/english/street_work_with_prostitutes.html.

5   *Lenke*, Fehér: Emberkereskedelem Magyarországon [Traficking in humans in Hungary]. In: *Póczik* Szilveszter - Dunavölgyi Szilveszter (szerk.): Nemzetközi migráció – nemzetközi kockázatok. HVGORAC, Budapest, 2008. pp. 425–445, p. 444.

6   *Mészáros*, Anikó: Rural poverty in Hungary drives the Western sex trade. Future Challenges, November 30, 2013. https://futurechallenges.org/local/hungarian-prostitutes-migrate-farther.

low levels of education, exploitation by traffickers and professional pimps.[7] The latter are in some cases older Roma women with backgrounds in prostitution, who even recruit prostitutes from their own clan, promising the girls well-paid hotel or restaurant jobs in Switzerland but their victims will be enslaved, abused and mishandled. Narcotized with alcohol and drugs, they are sent to the street and held under continuous control and financial and psychic pressure. They have to pay back their travel and supply costs as well as fictitious, non-existent debts. Those who are recalcitrant are told their houses in their homeland will be burned down or relatives, parents or children will be murdered etc. In the rare penal procedures, they are forced to perjury and false testimony, which is why neither the Police nor the NGOs, e.g. the Frauen Informations Zentrum[8] and its partner the Blue Point Foundation Budapest are able to offer effective help, although they do their best.

According to the report from the Solwodi Hilfsorganisation of Augsburg "more and more prostitutes from Eastern Europe come to Germany".[9] Young women aged 18 – 19 years from Rumania, Hungary and Bulgaria lured by so-called lover boys move to Germany in the hope to get good jobs and plenty of money. They are prostituted in brothels and rented apartments. As they are EU citizens, in lack of a denunciation or testimony reporting a crime – kidnapping, illegal captivity, forcing to prostitution etc. – the police is unable to undertake effective measures. In 2013 the Augsburg Police noticed some 150 new women in the red light milieu. The majority of them being not able to withstand the pressure by the traffickers and lacking tongue knowledge, social contacts, profession and job are not able to leave the scene. Many of them are forced by the traffickers to have sex without condom. Those who are ill or were broken through the frequent drug and alcohol usage as well as physical and psychical torture will be sorted out and substitute with new girls called "new meat" in the language of the underworld.

According to the definition in Section 192 of the Hungarian Criminal Code the trafficking in humans is recruitment, transportation, transfer, harbouring or receipt of persons forced by threat or coercion, abduction, fraud, deception, abuse of power or vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, with the purpose of prostitution or other forms of sexual exploitation,

---

[7] *Bakóczy*, Szilvia – Kinback, Szilvia: Futtatók markában – magyar prostituáltak Zürichben. Nők Lapja Café.http://www.nlcafe.hu/ezvan/20140423/magyar-prostitualtak-zurichben/.

[8] http://www.fiz-info.ch; and http://www.kekpont.hu.

[9] *Kirstges*, Christian: Immer mehr Prostituierte aus Osteuropa kommen nach Augsburg. Augsburger Allgemeine. 10. Juli 2014. http://www.augsburger-allgemeine.de/bayern/Immer-mehr-Prostituierte-aus-Osteuropa-kommen-nach-Augsburg-id30512282.html.

forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs.

Hungary is a source, transit, and also destination country for women, men and children subjected to trafficking in persons, specifically forced female prostitution and forced labour. Women and children of mainly Roma origin from north-eastern Hungary are subjected to sex trafficking. Sex trafficking victims in Hungary continue to be subjected to exploitation in street prostitution and in brothels disguised as bars or massage parlours. Women brought abroad are forced to work as prostitutes. They are subjected to everyday physical and psychical abuse. In some cases, Hungarian women have been lured into sham marriages to third-country nationals in the UK and Austria who exploited or forced them to prostitution.[10] Trafficking networks are run by Roma family gangs or organised criminals connected to red light milieus. Men from Hungary are subjected to forced labour domestically and abroad (UK, Netherlands and Spain). Labour recruiters transport men to architectural work and keep their salaries. Traffickers also recruit asylum seekers in shelters. Roma families specialized for criminality in poor rural areas force homeless men to perform domestic or agricultural labour. According to Europol, some 18 percent of the victims were Hungarian in the period 2009–2013.

According to data provided by the Ministry of the Interior and collected from a variety of institutions (Police, Prosecution Service, Office of Justice, National Crisis Telephone Information Service (OKIT), Victim Protection Service (KIH), Chance for Families Foundation) about 50–60 victims were identified in every year after 2010 (see table below). The majority of the victims were subject to sexual exploitation. The number of victims exploited abroad was 15 in 2011, 10 in 2012 and 24 in 2013. Three foreign victims were identified 2 from Romania and 1 from Thailand. From the 35 victims in 2014 were all Hungarians, 15 victims of sexual and 18 of labour exploitation. According to data for 2014, 22 victims were exploited within Hungary, in growing number elderly persons trafficked for domestic servitude and benefit fraud (par. 132). There has also been reported transnational human trafficking for the purpose of forced marriage to the United Kingdom and Austria.[11]

---

[10] Trafficking in persons Report. June 2014. Department of State, USA (HUNGARY – Tier 2), pp. 200–202: http://www.state.gOv/j/tip/rls/tiprpt/2014/index.htm.

[11] Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by Hungary. First evaluation round. Published 29 May 2015 by Secretariat of the Council of Europe Convention on Action against Trafficking in Human Beings (GRETA Group of Experts on Action against Trafficking in Human Beings). https://www.coe.int/t/dghl/monitoring/trafficking/Docs/Reports/GRETA_2015_11_FGR_HUN_en_w_cmnts.pdf.

Figure 1. Registered victims of trafficking in humans in Hungary 2011–2014.

Victims Year	Total	Women	Men	Children
2011	58	49	3	6
2012	68	58	1	9
2013	43	41	2	-
2014	35	26	7	2

Source: Official Criminal Statistics (ENYÜBS) of Hungary, data extracted by the National Institute of Criminology, Budapest

Hungary is party to every relevant international convention: the United Nations Convention on Transnational Organized Crime and its Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children; UN Convention on the Rights of the Child, Convention on the Elimination of All Forms of Discrimination against Women, the conventions on Forced or Compulsory Labour, Abolition of Forced Labour, Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour, Eur. Convention on Mutual Assistance in Criminal Matters and its first Additional Protocol; Eur. Convention on Extradition and its first two Additional Protocols; Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, CE Convention on Action against Trafficking in Human Beings. As a member of the European Union (EU), Hungary is bound by the directives No. 2011/36/EU of the European Parliament on preventing and combating trafficking in Human beings, No. 2004/81/EC, No. 2004/80/EC, No. 2012/29/EU etc. Trafficking in humans was introduced in the Hungarian Criminal Code in 1998 (section 175/B of the Criminal Code) but its definition was revised in Section 192 of the new Criminal Code, i. e. Act C of 2012, in force since 1 July 2013.[12] Other applicable provisions of the Criminal Code are section 193 on labour exploitation, section 196 on sexual exploitation, section 203 on child prostitution, section 209 paragraphs 46–47 on child labour. The 2005 Act CXXXV on Crime Victim Support as well as Government Decree 354/2012 (XII.13)

---

[12] Act C of 2012 on the (Hungarian) Criminal Code, http://www.refworld.org/pdfid/4c358dd22.pdf.

on the Identification Order of Victims provides accommodation, protection and assistance for victims. Relevant are also Act II from 2007 on the Admission and Right of Residence of Third-Country Nationals, and Government Decree 114/2007 (V.24.) on the Implementation of Act II of 2007. According to the Penal Code, particularly aggravating circumstances are holding the victim in captivity; using of force or threat of the same and perpetration in a criminal organization with accomplices, for commercial goals as well as the commitment against juveniles and children (par. 4-6, section 192). Paragraph 6 provides for prison sentences 5–20 years or lifelong imprisonment if the offence is committed against a child under 14, results in severe injuries or danger to life and/or is committed for the purpose of pornography.

After a preparing work provided by the Ministry of Interior, Ministry of Human Capacities, Ministry for Foreign Affairs, General Prosecutor's Office, Metropolitan Court of Budapest, National Bureau of Investigation, Office of Justice, National University of Public Service, National Institute of Criminology, National Crisis Telephone Information Service and National Police Headquarters a Government Resolution on the National Strategy against Trafficking in Human Beings (1351/2013(VI.19.) was adopted for 2013–2016.[13] This program substituted the former National Strategy against Trafficking in Humans.[14] The new strategy identified identification, protection as well as return and reintegration of victims, prevention, prosecution of perpetrators, co-operation of governmental and civil organizations as priorities. The National Anti-trafficking Coordinator at the Deputy State Secretary for EU and International Relations in the Ministry of Interior is responsible for the co-ordination. The National Co-ordination Mechanism on Human Trafficking has to achieve a coherent approach to combating trafficking and to brings together the public actors and the NGOs (see par. 22–25). Beyond the administrative organizations listed above also the National Institute of Family and Social Policy, the Chance for Families 2005 Foundation and Hungarian Baptist Aid, the UNHCR and IOM as well as the US and Dutch Embassies participate in the work that receives support from the Media Support and Asset Management Fund. On TV channel MTV1, the program "Stragglers" reports frequently on missing juveniles. The participating NGOs in the Roundtable on Human Trafficking run shelters and grant advocacy to victims. At the Na-

---

[13] 4-Year Plan Document Related to the Directive against Human Trafficking and the European Strategy towards the Eradication of Trafficking in Human Beings and Replacing the National Strategy against Human Trafficking 2008–2012, http://thb.kormany.hu/download/0/0d/a0000/17_National%20Strategy%20against%20Trafficking%20in%20Human%20Beings%202013-2016_EN.pdf.

[14] Emberkereskedelem elleni nemzeti stratégia 2008–2012 [National Strategy against Human Trafficking 2008-2012] http://emberkereskedelem.kormany.hu/download/3/d7/70000/Emberkereskedelem%20elleni%20nemzeti%20strat%C3%A9gia%202008-2012.pdf.

tional Bureau of Investigation (former called Directorate for Combating Organized Crime) a Trafficking in Humans Unit with 11 officers responsible for investigating trafficking cases with international components was established in 2004. This unit maintains close contact with the Crime Prevention Units of the Police of the single counties. The Victim Assistance Service operated by the Office of Justice constitute a network of offices in all counties offering assistance, legal aid and limited financial compensation to all crime victims.

According to the critics provided in the US Trafficking in Persons Report 2014 "the Government of Hungary does not fully comply with the minimum standards for the elimination of trafficking, however, it is making significant efforts to do so [. . .] despite the large number of [. . .] victims internally and throughout the EU, victim assistance remained low [. . .] The new criminal code entered into force in 2013 fails to fully comport with the definition of human trafficking in the EU Directive 2011/36/EU. [. . .] The new criminal code criminalizes many forms of human trafficking, but is overbroad because it does not require the use of force, the threat of force, or fraud to prove the basic offense of trafficking in persons. [. . .] the law's new definition of exploitation was not specifically tied to forced labour, forced prostitution, or child prostitution, instead, it defines exploitation as the abuse of power for the purpose of taking advantage of a victim, rendering the trafficking definition potentially much more expansive than the purposes of exploitation set forth under international law. [. . .] The minimal training of police on trafficking resulted in a lack of awareness and sensitivity towards victims."[15]

---

[15] Trafficking in persons Report. June 2014. Department of State, USA. *ibid.*

Part IV

Countering international Organised Crime Groups: 8th Research Conference on Organised Crime, 2015

The conference took place at the InterCityHotel in Mainz from 7 to 8 October on the topic of "Countering International Crime Groups – Challenges and Opportunities".

The conference shed light on international organised crime groups regarding their structures, function and threat potential. Special focus was put on research activities, the OC situation, different combating strategies, identified investigation bottlenecks and recommendations for improvement. This included discussion of Russian speaking organised crime groups in the U.S., Europe and Germany as well as their activities in cyberspace, mobile criminal groups and outlaw motorcycle gangs and Russian and Eastern-European cybergroups. Moreover, the role of Eurojust in combatting organised crime and the local dimension in combatting human trafficking and drug crime was presented. Practitioners and academics from the U.S., Great Britain, the Netherlands, Sweden, Switzerland and Germany and presented their viewpoints at the conference.

After the opening statement of **Martina Link**, the Director of the Criminalistic Institute at the Bundeskriminalamt, **Ursula Töttel** provided an overview on the project, including the yearly research conferences (see Part I "EU Project 'Research Network on Organised Crime' 2010–2016").

The relationship of OC in relation to the emergence of oligarchical fortunes in Russia along with the involvement of Russian OC in virtual illicit trade and the significance of Russian OC in international money laundering through global banking systems were the subjects of the presentation **"The Globalization of Russian-speaking organized Crime"** by **Dr. Louise Shelley**, Hirst Endowed Chair, University Professor as well as founder and director of the Terrorism, Transnational Crime and Corruption Center (TraCCC) at George Mason University.

Shelley clarified that she is concerned with new network-based OC groups emerging in the post-Soviet period. These groups are not hierarchically structured like mafia organisations, but rather collaborate due to a mutual economic interest. Moreover, they are composed of a vast variety of actors, ranging from high-rank government officials to corrupt facilitators who operate with flexible network structures. Shelly further stated that there are three reasons for the globalization of Russian OC: Firstly, the mobility of people, secondly, the movement of money through post-Soviet space and lastly, the leading role of Russian-speaking criminals in producing malware, spam, phishing etc. Referring to the link between the origins of oligarchical fortunes and OC, Shelley criticised that literature generally ignores this connection. Especially in

the UK, prosecution revealed the involvement of OC in creating oligarchical fortunes. Accordingly, 47 people were murdered in the aluminium industry. OC networks operate via sub-units outside of post-Soviet countries to plan their further approaches and dispose of assets. These criminals will most likely operate from countries with visa free or visa on entry policies because it is the easiest way for criminals to enter a country. Furthermore, a possession of property overseas empowers them to establish operation bases in the respective country. One could record that the facilitators of OC are "not the thug end of organised crime". Corruption nevertheless impedes the surveillance of who is entering the country. The movement of money through post-Soviet space is carried out by means of front companies and offshore accounts. Shelley reported that many banks do not do sufficient due diligence on their clients with respect to financial flows on their accounts which does make them accomplices in OC. She pointed out that centres of operations for OC are "the usual suspects" like Cyprus, Dubai and Moldova but also financial centres like Liechtenstein. Thereupon, Shelley deduced problems of countering this criminal activity: Some economies of members of the EU have become dependent on the money from criminal activities. The ways employed to disguise the origin of the money are eminently complex and require specific investigative resources. Another problem is posed by the corruption of officials who basically prevent any measures to counter OC from bearing fruit. At the end of her lecture, Shelley stated that there is a significant need for more network analysis as well as an extensive need for people with an understanding for the Russian language and culture.

Regarding the contribution to cross border investigations, work at different levels and the international coordination meetings, **Benedikt Welfens**, Senior Public Prosecutor, Deputy to the National Member of Germany and Chair of the Team Trafficking and Related Crimes from The Hague, gave an overview of the roots and development of Eurojust in his presentation titled **"The Role of Eurojust in combating organised Crime"**.

In the EU, there is an enormous variety of legal systems which naturally influence the combatting of international crime. Therefore, it is necessary to think about ways to ease the international cooperation which concluded in the concept of Eurojust. Accordingly, Welfens stated that justice usually acts slowly, especially with regard to the convention on Mutual Legal Assistance (MLA) between the member states of the EU. Moreover, the lack of cooperation concerning cross-border investigations is under criticism. Welfens continued to stress the contribution of Eurojust on an international level and described the practises used. He mentioned real, specific cases in order to clarify Eurojust's function within the EU. Thus, Eurojust is working at three different levels: firstly, a plenary meeting, secondly, involving only national desks, thirdly, investigators/prosecutors/judges dealing with specific cases.

Various third states, cooperation partners and international organisations such as Europol, which is the largest participant in such meetings, are involved in coordination meetings. In addition, priority crime areas consist of 65%, including fraud, drug trafficking, (mobile) OC, crimes against the financial interests of the Union (PIF crimes)[1] etc., whereas 35% are graded as non-priority crime areas. Another important value of Eurojust is the funding of Joint Investigation Teams (JIT's)[2] since financial or organisational constraints connected to the international character of crime should not prevent their largely necessary involvement. Furthermore, the involvement in funding these teams also enables Europol to gather information on specific cases as well as evaluating the effectiveness of JIT's. An additional task of Eurojust is considered to be the enhancement of cooperation and exchange with e.g. Europol and other third states through coordination meetings and coordination centres. Moreover, Welfens presented a case example of trafficking in minors for committing theft: A Bosnian criminal network trafficked underaged Bosnian girls who committed theft, mainly on the Parisian public transport system. The Prosecution Office in Paris requested Eurojust assistance in coordinating the investigations ongoing in France and Bosnia-Herzegovina. Two coordination meetings were set up, bringing the involved authorities together in The Hague and Sarajevo. The French-Bosnian cooperation included joint investigations, surveillance, telephone interceptions and securing searches, seizures and arrest warrants. Judicial authorities, police, NGOs, institutions in charge of legal child protection in France and Bosnia-Herzegovina and Eurojust worked closely together to make this operation a success.

As a result, the involvement of Eurojust in a given case may support the investigation by funding joint teams, for instance, by accelerating the MLA and JIT's, by connecting networks, by providing useful information, by coordinating actions of legal authorities with regard to searches, arrests and confiscations and last but not least, by avoiding misunderstandings due to diverse legal systems.

The second day of the research conference commenced with a presentation by **Johan Lundberg**, Superintendent at the Swedish Police Authority in Gothenburg, Sweden. In his presentation entitled **"Mobile Eastern European Groups in Sweden – Project Metal Thefts"**, two police operations, "Kopparorm" and "CIRCA", as well as their planning, execution and results were outlined.

---

[1] From the French "protection des intérêts financiers".

[2] According to Europol: "A Joint Investigation Team (JIT) is an investigation team set up for a fixed period, based on an agreement between two or more EU Member States and/or competent authorities, for a specific purpose. Non EU Member States may participate in a JIT with the agreement of all other parties."

"Operation Kopparorm", which is concerned with metal thefts, was introduced due to the police district of Örebro reporting that metal thefts posed a growing threat to local authorities in 2004. Accordingly, the Police Authority of Västra Götaland investigated the cases and published a report which then became the basis for "Operation Kopparorm" in 2006. The investigation led by the Police Authority of Västra Götaland clarified that metal theft poses a public danger as well as endangering the infrastructure. The analysis revealed that companies in Gothenburg had purchased stolen metal from thefts all around the country and as there were no receipts or cash payments existent, the identification of sellers largely could not be conducted and was inadequate. Consequently, it was necessary to cooperate with other authorities for instance the tax authority, the eco-crime authority and insurance companies. Moreover, the proposals also included measures for crime prevention, such as effective locks and legislative amendments. Specific measures that should be taken include: the surveillance of the environment (via municipality), meetings with industry representatives, and audits of tax agencies. As a result, in 2011 there were convictions of five people who belonged to a larger group of metal thieves. The leaders were originated in former Yugoslavia and the "doers" were of Romanian extraction, all receiving sentences of 25 years in prison and stole money in value of 2.5 million Euros due to tax crimes and organised crime. According to Lundberg, key factors for succeeding are a national focus and a group with national responsibility, cooperations with other authorities such as the groups in Munich, London, Finland, Norway and Denmark, but also obtaining the necessary resources for investigation as well as intelligence personnel, specifically focusing on Europol, which reinforces the persistence on metal theft crimes. The "CIRCA" unit came into life in 2009, is originated in Gothenburg and Vårgårda, and focuses on a distinct investigative and international perspective. Perpetrators are identified as participants of Mobile Organised Crime Groups (MOCG), who often come from Bulgaria and Romania and are notably known for various criminal offences in Europe, such as shoulder surfing[3], pickpocketing and robberies. In many cases the group members are not known for their current criminal activities in their home countries, although they do have a criminal record. On average, ten MOCG's are convicted per year and consist of two to four people, whereas nearly half of the convicted members are from Romania. Each MOCG can be linked to 20 to 30 offences, and most interestingly, approx. earn 1,000–1,500 Euros per theft.

---

[3] Shoulder surfing is a security attack where the attacker uses observation techniques, such as looking over someone's shoulder. This is commonly used to obtain passwords, PINs, security codes, and similar data.

The presentation, **"The local Dimension in the Containment of international organised Crime: The Dutch Example"**, given by **Prof. Dr. Cyrille Fijnaut**, professor of International and Comparative Criminal law at Tilburg University in the Netherlands, focused on the history, context and containment, specifically through the Emergo project which aims at combatting organised crime through targeting criminogetic sectors as well as it supports the collaboration of research and analysis to understand the extent of organised crime, of the OC problem in the Netherlands and more specifically, in Amsterdam.

Firstly, Fijnaut referred to historical developments within OC, such as banditry and urban underworlds. In more detail, the concept of the international criminal who, due to urbanization and the train system was able to operate from various countries and exploit new sectors was outlined. Hence, the international criminal operated across borders which evoked the need of identification systems. As there is a common debate upon the actual definition of OC, there are some people who favour the view that the focus lies on people forming networks and engaging in criminal activities, but there are also those who state that the activities carried out form the character of OC, not the constellation of people. Fijnaut continued to outline the nature of the problem in terms of people and in terms of activities. With regard to activities, he claimed that there are a lot of similarities between the EU countries concerning the delivery of goods and services on black markets. Nevertheless, there are local differences regarding the illegal control of legitimate markets. As the topic of transnational OC was also raised multiple times during the conference, Fijnaut assessed that with regard to the situation in Amsterdam, OC is to some extent not transnational, for OC stays in the inner city as was also made visible by the example of the La Cosa Nostra in New York. The transnational dimension is reached through crossing the border from Manila to Amsterdam and hence the need for organised criminals to establish a good communication system. Additionally, it was pointed out that "transnational OC" was commonly used as a term in order to neutralize the implication of OC and not exclusively focusing on "traditional" countries of OC such as Italy or Colombia. The transnational level of OC should not only be recognised, but rather the local dimension as well because if the local authorities do not counterfeit OC, the problem will never be able to be curtailed. One possible method for containing the problem was already conducted in the US, especially in New York: It involves the issuance and also the withdrawal of licences in order to clean legitimate markets. Moreover, it was affirmed that the real power is still located within local authorities and that, as the example from New York reveals, knowledge of criminal law can be used for administrative purposes. The hard core of the problem was further illustrated by the fact that mayors as well as public official are being threatened and intimidated by OC because they established as system of screening in keeping with the New

York model. Furthermore, Fijnaut clarified that not only the people being actively involved in organised criminal activities would have to be pursued, but also the people enhancing and profiting from OC. This was illustrated by the example of Philips selling light bulbs to people who actively operated in the cultivation of cannabis and thus enhanced the illegal cultivation of cannabis. The illegal cultivation of cannabis and the production of synthetic drugs form the greatest problem in the Netherlands, since it was determined that nearly 3,000 people are involved in the illegal cultivation of cannabis on a daily basis. This led to the next topic in Fijnaut's presentation, which was focused on the current debate on the legalization of cannabis in order to curtail the OC problem in this respective field. On the one hand, the legalization of cannabis would be a profitable way to gain money as well as an effective measure to combat OC, but on the other hand, the Netherlands cannot do this individually. It was suggested that the legalization should take place in a European framework, maybe also including Germany. Additionally, Fijnaut lined out specific measures in Amsterdam to define, reduce and curtail OC because of the urgent need for methods to counter OC in the Netherlands. Such measures included the Emergo project, the establishment of special departments as well as first research into the field of OC in Amsterdam by the Research-Group Fijnaut, which aimed at identifying the "intertwining" between OC and the legal economy. The plan consisted of regaining control over the real estate market, applying screenings for licences, and overall, the reduction of opportunities in criminogetic markets.

Wilbert Paulissen, the Chief Superintendent and Head of the Central Criminal Investigations Division in Driebergen, NL, gave a lecture entitled **"Countering Outlaw Motorcycle Gangs in the Netherlands"** which focused on the development of Outlaw Motorcycle Gangs (OMG) and the respective measures and approaches of the authorities to counter the issue.

Firstly, the importance to address the topic of OMGs was briefly examined, for the OMGs in the Netherlands and Germany influence each other. Next, Paulissen gave an insight into the goals, problems and approaches of the Dutch National Crime Squad (DNR) and the Dutch National Police. The DNR combats international OC and is currently focused on the problems in the South of the Netherlands, fights terrorism and investigates in cases of national interest. On January 1, 2013 the former 25 regional police forces and the Dutch Police Services Agency (KLPD) merged to become a single national police force. A new approach was established due to the increase of criminal assassinations in the Netherlands. The approach includes the belief that not solely criminal investigations will harm international OC, but that the police authorities would have to cooperate with the local government, which is now more interested in OC than it was before as well as working together with private companies. Moving on to the original topic of OMGs in the

Netherlands, background and data were presented. The police authorities focused on a multi-agency approach and it was examined that formerly, there was a council of nine OMGs talking about their problems in order to prevent conflicts among them which is quite important because otherwise, it would call the attention of the government. This council ceased to exist in 2013 as the "Satudarah" previously left the council which was related to Germany since the Hells Angels claimed to be the only international OMG. Therefore, the awareness within the authorities of an upcoming problem was raised, as it was commonly perceived when two international OMGs exist in one country, a motorcycle gang war is likely to commence. Moreover, the statistics shown projected that in 2015 the "Satudarah" could increase its chapters to 79 chapters in 90 countries, but also the supporter groups have risen enormously. As a result, the goal of decreasing the chapters was not reached. Accordingly, Paulissen went on to summarize the background of the "Satudarah" and also noted that in the first 20 years of their existence, there was no vast growth, whereas after they left the council the growth expanded exponentially. Also, it was assessed that OMGs such as the "Satudarah" or the "No Surrender" increasingly make use of the media to impress society. One of the approaches of the Dutch police authorities includes contacting, examining and questioning the people who are involved in the media advertisement of the OMGs, as Paulissen warned not to underestimate these groups. With reference to the aforementioned assumption of an upcoming biker war, it was stated that there were a number of incidents which confirmed the concern. With the example of the newly established "Bandidos" in the Netherlands, who only had few chapters, police authorities decided to stop the OMG and started investigations in cooperation with regional forces, resulting in the conviction of several members. This preventive measure stopped the growth of the "Bandidos" in the Netherlands. The closing of clubhouses led to the threatening and intimidating public officials, especially mayors, further Paulissen stated that it is important to act as "one" government in order to deal with the problem.

The presentation on "**Eastern European Cybercrime Groups**" by **Prof. Dr. Federico Varese**, Professor of Criminology in the Department of Sociology at Nuffield College, examined a framework for understanding organised crime with respect to two case studies on the Russian cyber underground and his field trip to Ramnicu Valcea, the capital city of Valcea County, Romania, which is considered a hub of cybercrime in Europe.

He pointed out that there is a vast confusion regarding the meaning of OC originated by the United Nations (UN) definition for it is too vague for developing hypotheses. Varese stated that he prefers to use concepts which have proven useful in mainstream sociology, politics and economics, namely: production, trade and governance. As much as in the "legal" world, there are people in the illegal world who are involved in the production of goods and

services. In addition, there are also people who move these produced goods into various cities and countries, usually referred to as trafficking. The third type of activity is often misunderstood: people who do not just sell and move their goods, but they gather their goods in order to decide who is allowed to produce and trade. Furthermore, Varese claimed that this is exactly the occupation of the government with regard to a legal viewpoint as it tries to impose a natural monopoly over their ambiguity to govern. In particular, he stated that the latter type of people is commonly disregarded, which is quite dangerous as these people enormously differ from people who produce or trade in the illegal world. With regard to production, he referred to a case which involved the production of cocaine in Colombia whereby the cocaine was put into tuna cans and was then transported to Calabria. Moreover, they developed a "branding" of the cocaine which also served the purpose to build a reputation for the goods as a key element to trade. Furthermore, another way of ensuring cooperation across long distances in the absence of trust is assumed to be hostage taking. In addition, he assessed his first topic: the 'Russian Underworld'. The first question raised concerned the extent of the Russian Underworld, which he measured by counting and estimating the number of forums depending on their activity. The number is perceived to be within the range of 60 to 78 forums with up to 220,000 users. Next, it was elaborated on the goods which are traded in these forums, namely malicious code uploads, router exploitation, mobile phone attacks and money laundering with regard to the purchase of corporate accounts in the US, Germany etc. This was also referred to as bulletproof hosting, as one goes to a website to buy a secure server to store illegal data such as pornographic material. Moreover, one can also buy escort services in case of trust issues regarding a partnership. Varese also called attention to the fact that the prices for the respective services are quite low, which hints to a flourishing market, well governed by the forum administrator. Furthermore, new marketplaces have developed, since new automated forums with standardized services have been established so that there is no need to engage in long forum discussions. Varese also examined the impact of the Ukrainian crisis on the cyber Russian world: Firstly, he hinted at the most important rule within the community not to attack the Russian speaking community. With the recent developments in the Ukraine, there seems to be a split within the community which is divided into pro-Ukraine and pro-Russia; this evokes the possibility of attacks in Russian-language cyberspace and could reinforce "hacktivism". Regarding Ramnicu Valcea, Varese claimed that there is an extremely strong local dimension, which allows these cyber criminals to thrive which is the reason he went on a trip to untangle this mystery. Furthermore, it was pointed out that Ceauşescu invested in IT, programming etc. and reinforced a rich culture of engagement with technology. So is it really true that Ramnicu Valcea is the hub for European cybercrime? Varese assessed this question by referring to fraud cases in Romania.

The majority of scams in Ramnicu Valcea involve customers from the UK whereby a fake offer is posted on platform like eBay, the UK shopper buys the goods and transfers the money to an UK bank account, which is then withdrawn by an "arrow"[4] and transported to Romania. Most of the scammers attended a specific school for IT skills and were introduced to this criminal field by their teacher. In conclusion, Varese stated that these cyber criminals are protected by the corrupt local police and administration.

In his lecture titled **"Corruption Threats in Southern Eastern Europe"**, **Ambassador Dr. Uglješa Zvekic**, Senior Advisor in the Global Initiative against Transnational Organized Crime in Geneva, addressed the connections between corruption and organised crime from a theoretical level to a South Eastern European perspective.

Zvekic stated that corruption is assumed to be one of the main threats to legal, economic and political stability and that organised crime uses corruption as a means for carrying out their illicit trade as well as legalising their money and escaping the justice through e.g. investing in legitimate businesses. Firstly, new trends in crime have been outlined: Threats and risks of crime in general have increased over time and remarkably, as violent crime declines, global OC and corruption seem to increase. This tendency naturally fuels an increase in international legal responses and cooperation; although OC is not a new phenomenon, its extent has rapidly expanded. Introducing his main topic, Zvekic examined that corruption has been politically acknowledged through Transparency International's (TI) Corruption Perceptions Index (CPI) on an international level. Nevertheless, he focused on his countries of origin in the Balkan region and states that non-EU countries can make use of the CPI to control and weaken their problems in public administration. Moreover, Zvekic applied multiple surveys by TI and the UNODC to illustrate the vulnerability of institutions to corruption. As a result, it could be recorded that the highest levels of corruption occur in political parties, public administration and the police, thus in institutions which are normally thought to exercise control and maintain the order of the system. Zvekic additionally recalled that these threats are already real and will only increase in the future if they are not contained properly. Zvekic clarified that the political influence on police force within states like Serbia is very high. He also warned that bribery within the police force poses a very serious weakness, hence police reforms like strengthening the accountability and diminishing the corruption would be necessary.

---

[4] Refers to a gang courier.

OC in the Balkan region is, as is affirmed by Zvekic, more a group activity rather than a single operation. Due to the fall of the Berlin wall, the Balkan region experienced a "wild-west" privatization leading to the establishment of OC in the "new world". Another key focus in Zvekic's presentation lay on the legalization of criminal profits, as laundering the illicitly gained money is in itself also a process of legalization. Measures to counteract money laundering are already at hand, although the fact that OC starts to buy shares in companies will pose a much bigger problem as cooperations with the corporate sector are increasingly necessary. In conclusion, he stated that public works as well as the privatized economic sector enhanced the spread of OC in the Balkan region. Thus, in opening up the market for new investments, OC is able to buy its way into a legal presence in society. Therefore, the improvement of public administration, public bits and monitoring is of such importance, as the police usually interferes when the deed is already committed.

In his presentation on **"Eurasian organised Crime Structures in Germany – Countermeasures and Efforts of German Law Enforcement Agencies"** **André Schünemann**, Kriminalhauptkommissar (Detective Chief Inspector), M.A., at the Bundeskriminalamt (BKA) in Wiesbaden presented current measures of German law enforcement agencies to counter the establishment of Eurasian organised crime in Germany, especially with regard to Georgian burglars and shoplifters, who are supervised by professional criminals.

Firstly, basic information on Eurasian OC was examined which then followed a description of project JASON which is concerned with Georgian OC structures. In closing, he talked about the approach the BKA has developed in order to curtail OC. The 'thieves-in-law' are mainly career criminals from the top in the hierarchy of the Russian-Eurasian OC. Correspondingly, the situation in Germany was illustrated with reference to the number of Russian-speaking population, namely 4.5 million, in relation to the total number of inhabitants of Germany. Between 4,500 and 5,500 prison inmates in German penal institutions subject themselves to the code of the thieves-in-law. Russian-Eurasian OC groups are mostly invisible to the citizens and sometimes also to the police, unless their criminal activity becomes public. Offenses of Georgian OC groups, such as property crime, fraud, money laundering and investment in legal businesses were illustrated by examples in Germany. The difficulty is verifying the Georgian shoplifters' ties to the criminal structures of Russian-Eurasian OC. However, reports from several federal states are in agreement that Georgian nationals registered in Germany as asylum seekers are active in these fields of criminal activity. Within the scope of the Project JASON, it was hinted at the fact that Georgian gangs of shoplifters and burglars in Europe operate under the protection of Georgian thieves-in-law. Therefore, it has become an obligation for the BKA to take action against Georgian OC groups at national level and on a long-term basis. The project's

goals include the destruction of Georgian OC structures and logistics, the establishment of evidence for Georgian petty criminals being led by thieves-in-law, the establishment of a nationwide network fighting crime and the enhancement of international cooperation. In accordance with the aim of coordinating activities at both national and international level, Europol, Interpol but also countries of origin as well as countries who suffer as a result of Georgian OC, are important partners in the fight against OC. A further focus was then placed on Project MILLENNIUM, which refers to Interpol cooperating with 45 member countries on collecting and processing information concerning Russian-Eurasian OC. Germany, as a Co-Driver, will support and promote this work over the course of a year. As new crime phenomena and dynamic challenges occur, the responsiveness of police authorities is also challenged and demands a new concept for fighting OC which is based on an analysis and investigative projects. Accordingly, a coordination unit was established for organised crime which quarterly enquires actual working topics at federal and state or 'Länder' level and coordinates the cooperation of the concerned agencies and strengthens the national and international communication. The identification process of common fields of activity was then presented and enclosing important questions like what perspectives Project JASON can offer with regard to future crime suppression efforts were raised.

Outlook

At the present time we are trying to get EU funding for a follow-up project. But in 2016 we will not have a research conference. We intend to maintain the OC Research Network and to hold conferences in the future as well. Henceforth, conferences should also be conducted on selected phenomenological topics with international relations.

The Globalisation of Post-Soviet Organised Crime

Louise Shelley

George Mason University, Fairfax, U.S.

Post-Soviet organised crime has been globalised in diverse ways. It has not achieved this global reach by the movement of organised crime to new locales such as was seen with the traditional Italian mafia that moved from Italy and took root in such new locales as the United States, Canada and Argentina. The failure of traditional crime groups out of the USSR to migrate success-fully has been well documented.[1] Instead, the post-Soviet crime groups that developed rapidly after the collapse of the USSR have become important ac-tors in contemporary transnational crime.

Post-Soviet organised crime is characterised by mobility, the movement of large amounts of money through banks and financial institutions, particularly in countries such as Moldova and Latvia. According to Global Financial In-tegrity, between 2010 and 2012, an estimated \$141 billion illicitly flowed out of Russia annually.[2] The exodus of illicit capital is closely correlated with the growth and endurance of the underground economy.[3]

Yet criminal activity also affects capital flight in other ways. The inability of citizens to protect their assets from the predatory activity of Russian crime groups or that of corrupt high-ranking officials has also been an important force motivating the departure of money from Russia since its independence.

Russian organised crime is a less visible presence within Russia than in the early 1990s when the thuggish element of the organised crime world was so in evidence in the restaurants, hotels and markets of Russia. The rise of a stronger state under Putin has left less capacity for Russian crime groups to operate openly and some specialists have suggested that the central govern-ment has co-opted organised criminal activity making it a less independent force.[4]

---

[1] Federico Varese, *Mafias on the Move: How Organized Crime Conquers New Territories*, Prin-ceton: Princeton University Press, 2011.

[2] Dev Kar, Russia: Illicit Financial Flows and the Role of the Underground Economy, in *Illicit Financial Flows: The Most Damaging Economic Condition Facing the Developing World*, Washington, D.C.: Global Financial Integrity, 2015, 77.

[3] Ibid., p. 86.

[4] Karen Dawisha, *Putin's Kleptocracy, Who Owns Russia?,* New York: Simon and Schuster, 2014.

But if Russian criminals are less evident on the streets, they have moved into another arena. Russian organised criminals have become key actors in the globalised world of cybercrime and perhaps the most active producers of spam on the Internet as well as the sellers of many products key to the commission of cybercrime.[5] The prevalence of Russian criminals in transnational cybercrime activity is explained by multiple factors: the technical capacity of the criminals, the absence of legitimate outlets to employ their skills within Russia and the failure of the Russian to effectively counter cybercrime. In fact, there are indications that some Russian-speaking cyber criminals are allowed to continue to operate because they provide service for the state. This follows a model that has existed from the Stalinist period in which ordinary criminal prisoners in labour camps did service for the state by keeping the political criminals in line. Today, service to the state extends beyond the labour camps to the global cyberworld.[6]

1   Structure and Composition

Russian-speaking groups are composed of members of different successor states from the former Soviet Union. Often, the older members of these organisations met while they were incarcerated together or met while they served in the Afghan war. Therefore, shared experiences are more important in shaping the compositions of groups than familial and ethnic ties.

The organised crime groups that developed in the final years of the Soviet period do not have permanent membership and induction rituals as exists with mafia type organisations. They also differ in these respects from the traditional *vory-v-zakone* or thieves-in-law, the organised, who existed from the pre-revolutionary period and was not totally wiped out by the Soviet authorities.[7]

Rather, contemporary post-Soviet organised crime may involve a wide range of actors including: high-ranking government officials, corrupt law enforcement, ordinary criminals, bankers and corrupt facilitators who operate with

---

[5] Brian Krebs, *Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door*, Naperville, Ill: Sourcebooks, 2014.

[6] Owen Matthews, *Russia's Greatest Weapon may be Its Hackers*, May 7, 2015, http://www.newsweek.com/2015/05/15/russias-greatest-weapon-may-be-its-hackers-328864.html, also interviews with American law enforcement.

[7] Valery Chalidze, *Criminal Russia: Crime in the Soviet Union*, New York: Random House, 1977; Frederico Varese, *The Russian Mafia: Private Protection in a New Market Economy*, Oxford: Oxford University Press, 2005.

flexible network structures.[8] It is these attributes that allow them to commit a diverse range of offences including large-scale cybercrime, transnational fraud and money laundering.

Russian-speaking criminals cooperate in their criminal activities with citizens of other Soviet successor states. Illustrative of this is a well-mapped human trafficking case in the United States, where participants came from Russia, Ukraine and operated in the Baltics as well.[9] Other criminal networks may contain both Azeris and Armenians, although these countries do not have diplomatic relations.

Political conflicts rarely appear as an impediment to criminal associations.

The Russian invasion of Crimea has not ruptured the cooperation of all Russian and Ukrainian criminals. Rather, crime has flourished in Crimea since the invasion. The conflict instead provided new criminal opportunities.[10] Financial interests often trump nationalist sentiments as organised criminal groups prioritise making money.

Post-Soviet groups differ from many more traditional criminal groups because they are flexible and are extremely adaptive to changes in circumstances. Groups that are controlled by Slavic as opposed to Caucasian groups are often not hierarchical in nature. They do not consist of family-based organisations but are comprised instead of flexible network structures. These generalisations apply to criminal groups that engage in more traditional forms of criminal activity such as the drug trade, human trafficking and financial fraud. But it is particularly true of the more specialised Russian-speaking criminals who operate in the cyber world. These new crime groups are based on their technological skills and ability to gain money illicitly rather than the personal ties that are often preeminent in more traditional groups that operate in the real world.

2   Education and Capacity to Globalise

The high educational levels of the former Soviet Union have also contributed to the globalisation of their activities. Many criminal groups include former

---

8   Louise I. Shelley, Contemporary Russian Organised Crime: Embedded in Russian Society, in *Organised Crime in Europe: Patterns and Policies in the European Union and Beyond* (eds. Cyrille Fijnaut and Letizia Paoli) Dordrecht: Springer, 2004, 563–84.

9   *White Lace Case*, http://www.lapdonline.org/january_2003/news_view/21690, the author has seen the network map developed for this case.

10 Robert Orttung and Christopher Walker, *Putin's Frozen Conflicts*, February 13, 2015, http://foreignpolicy.com/2015/02/13/putins-frozen-conflicts/.

members of the security apparatus who had extensive language training and overseas operational experience including the requirement that they move money abroad for Soviet operations. Therefore, these individuals have the capacity to function globally. Also the presence of senior corrupt officials as direct participants and/or facilitators of crime groups means that they also often have the training to function effectively outside the Soviet Union. They have the sophistication to open overseas bank accounts, buy property abroad and function in a global economy.

The impact of high educational levels and technical training are most evident in the competitive edge that Russian-speaking organised criminals enjoy in the cyberworld as will be discussed subsequently.

3   Russian Organised Crime and the Legitimate Economy

Russian-speaking organised crime has consistently been involved in the legitimate economy and not just with traditional criminal activities such as the drug trade, prostitution and gambling. Russian organised crime early on decided that it could make a fortune by being involved in the privatisation of state property. It acquired this property for itself but also played a key role in the consolidation of fortunes of many who became oligarchs during the process of privatisation.

Yet this role of organised crime has not been recognised much in the west as most of the literature on the rise of oligarchs ignores the role of crime groups in the acquisition and retention of key properties that once belonged to the state.[11] The only noted exception to this is the work written by Paul Klebnikov who analysed the role of organised crime in the rise of an oligarch. He was murdered in Moscow, probably as a result of his writing.[12]

Litigation, particularly in Great Britain, has revealed the role of organised crime in the consolidation of fortunes, particularly in the aluminium industry. Forty-seven people were murdered before ownership of key production facilities was achieved and sustained by several oligarchs.[13]

---

[11] David E. Hoffman, *Oligarchs: Wealth and Power in the New Russia*, New York: Public Affairs, 2011; Chrystia Freeland, *Sale of the Century, Russia's Wild Ride from Communism to Capitalism*, New York: Crown Business, 2000.

[12] Paul Klebnikov, *Godfather of the Kremlin: The Decline of Russia in the Age of Gangster Capitalism*, New York: Harcourt, 2000, https://cpj.org/killed/2004/paul-klebnikov.php, notice of Klebnikov's murder.

[13] Jane Croft and Catherine Belton, Deripaska Reaches out-of-Court Deal, in *Financial Times*, September 27, 2012, http://www.ft.com/cms/s/0/34715a84-cb72-11e1-916f-00144feabdc0.html#axzz3p5JcmLcl, accessed October 20, 2015.

Many Russian fortunes were not secure because law enforcement bodies and the courts did not adequately protect rights. In one new form of criminal activity, dubbed corporate raiding, members of the police and judges were often part of the scheme that wrested valuable property and businesses from their owners –a phenomenon defined as "corporate raiding."

The widespread problem of "corporate raiding" developed in Russia and other Soviet successor states after the first wave of privatisation of state property.[14] Corporate raiding was generally initiated by economic rivals and corrupt officials. But the likelihood of a raid was enhanced if an oligarch fell out of political favour. A much broader range of entrepreneurs and businessmen were subject to corporate raids than the relatively limited number of oligarchs.

Corporate raiding is described as follows:

'Reiderstvo' differs greatly from the U.S. hostile takeover practice in that it relies on criminal methods such as fraud, blackmail, obstruction of justice, and actual and threatened physical violence. At the same time, though, 'reiderstvo' is not just simple thuggery. In contrast to more primitive criminals, Russian 'reideri' rely on court orders, resolutions of shareholders and boards of directors, lawsuits. In short, it is a new more sophisticated form of organised crime."[15]

The threats described above were often carried out by organised crime and therefore it is hardly surprising that corporate raiding often involved significant threats to the life and welfare of individuals whose property is sought by highly protected and connected individuals."[16] It emerged as a phenomenon in the 1990s, intensified in the 2000s and still continues.

The director of the Audit Chamber of Russia, Sergei Stepashin, reported in 2009 that there were 40,000 cases of raiding annually in different sectors of the economy throughout Russia. Of these, only fifty-five were investigated, according to President Medvedev.[17] Some Western sources estimated the

---

[14] Thomas Firestone, Criminal Corporate Raiding in Russia, in *The International Lawyer*, Vol. 42, No. 4, Winter 2008, 1207–29.

[15] Ibid., 1207.

[16] Louise Shelley, Crime, Organized Crime and Corruption, in *Return to Putin's Russia*, 5th edition (ed. Stephen K. Wegren), Lanham, Maryland: Rowman and Littlefield Publishers, 2013, 194.

[17] Maria Antonova, *Kremlin Tightens Screws on Corporate Raiders*, May 14, 2010, http://www.themoscowtimes.com/business/article/kremlin-tightens-screws-on-corporate-raiders/405960.html, accessed November 29, 2014.

number of raiding cases as high as 70,000 annually.[18] This reveals the almost total impunity of the raiders.

It is the pervasiveness of this corporate raiding that has made many wealthy Russians move their money overseas. For example, Khodorkovsky's Yukos company was raided after the oligarch fell out of political favour. Khodorkovsky was incarcerated for a decade and lost title to his company.[19] Only in 2015, a decade after this corporate raid, did international courts rule in his favour. Seeing the example made of Khodorkovsky, many Russians have chosen to move their assets overseas.

Yet raiders also move their assets overseas. The well examined case of the raid against the Hermitage investment company was carefully documented by a report released by the Parliamentary Assembly of the Council of Europe which provided a detailed analysis of the corruption, organised crime and money laundering associated with a series of alleged corporate raids against the company and the subsequent fraudulent filing for a multi-million tax refund. The Council of Europe report also revealed the multi-million dollar property allegedly purchased overseas by participants of this crime.[20]

4 The Globalisation of Russian Capital and Criminal Capital

Capital flight from Russia has been such a significant problem because of the insecurity of property rights, the absence of a rule of law and an independent judiciary. These are structural problems of the Russian state rather than consequences of the presence of organised crime. But organised crime has contributed in an important way to the movement of money overseas.

Many policies exist in different regions of the world seeking foreign capital that have made it easier for Russian-speaking organised crime to globalise its activities. Russian-speaking crime groups are not the only ones to take advantage of this ease of entry but they have made significant use of it. Visa free regimes or visas received on entry mean that members of Russian-speaking organised groups can easily enter countries such as UAE, Cyprus and Turkey. They have become key locales for the movement of people and also licit and

---

[18] Luke Harding, Raiders of the Russian Billions, in *The Guardian*, June 24, 2008, http://www.guardian.co.uk/world/2008/jun/24/russia.internationalcrime, accessed November 29, 2014.

[19] Richard Sakwa, *The Quality of Freedom: Khodorkovsky, Putin and the Yukos Affair*, Oxford: Oxford University Press, 2009.

[20] Andreas Gross, *Refusing Impunity for the Killers of Sergei Magnitsky*, November 18, 2013, Council of Europe, Parliamentary Assembly, http://www.assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20084&lang=en.

illicit money. Countries of the former Soviet Union, such as Latvia and Moldova, are key locales for laundering money. Latvia, despite its membership in the European Union, has been a key conduit for the movement of illicit funds.

Large bank accounts with laundered money from the former Soviet Union have been found in key financial centres in Europe as well as in the United States. In the late 1990s, the Bank of New York was found to have moved large amounts of money tied to Russian organised crime. Unfortunately, this is not a phenomenon confined to the previous century but has been associated with major international banks in the 2000s as well that have not performed adequate due diligence on their clients or have turned a blind eye to the source of large funds. Money has been laundered in both Russian and foreign banks believed to be associated with Russian organised crime activity.[21]

The laundered money is found not only in banks but is laundered into property in many locales. Among the most known of these are Dubai, Cyprus, Turkey, the South of Spain and France, London and New York.[22] Yet the money goes east as well as west. The beach resort of Pattaya in Thailand has become a favourite locale for both licit and illicit Russian funds. Often these properties are not directly owned by individuals but are purchased through front companies. The possession of this property provides not just a place to park and enjoy one's money but also may give the criminals bases from which to operate overseas.

5   Movement of People

Traditional Russian-speaking organised crime began to move outside the Soviet Union in the 1970s and 1980s. At this time, the Soviet Union severely restricted emigration. However, certain ethnic groups were allowed to leave. Russian officials seemed particularly willing to allow individuals with criminal backgrounds to leave. Therefore, the interests of the criminals to leave and the desire of the state to get rid of them coincided.

The Armenian emigration to the United States included a small subset involved in criminal activity. Many of them settled, along with the law-abiding migrants, in Los Angeles. Criminal investigations and trials refer to the presence of the "Armenian power gang", a group tied to this emigration during

---

21 US Department of State, INCSR, Vol. II, 2011, 157.
22 See Ed Caesar, House of Secrets, in *New Yorker*, June 1, 2015, 22–30; William H. Byrnes and Robert J. Munro, *Money Laundering, Asset Forfeiture and Recovery, and Compliance –A Global Guide*, Thomas Jefferson School of Law, 2011.

the Soviet period.[23] The only significant other ethnic group permitted to emigrate from the USSR were Soviet Jews, who were permitted to emigrate to Israel. With emigration to Israel being the only viable means of exit, many serious criminals purchased fraudulent documents alleging Jewish ancestry in order to move to Israel and acquire citizenship that was automatically granted under the law of the return. Illustrative of this problem is Anton Malevsky, the reputed head of the Izmailovsky Group, who died in a parachuting accident in South Africa.[24]

The possibilities for movement expanded greatly with the collapse of the Soviet Union and the criminals readily took advantage of this opportunity. Organised crime groups moved to Eastern Europe with the end of Communism in Eastern Europe. Criminal groups such as the Solnstevo group and its leader, Semyon Mogilevich, established a base in Hungary. The perceived severity of this threat led to the establishment of an FBI office in Budapest to address the spread of Russian-speaking organised crime.[25]

Post-Soviet organised crime has moved to many more locales as revealed by many criminal investigations in the United States and Western Europe. Particularly prominent among these are large scale investigations of Russian-speaking crime groups in Spain and Italy. The Spanish case involved the arrest of a group connected with a Georgian thief-in-law that was involved in construction projects, extortion and also fraud. The Italian case has been analysed in Frederico Varese's *Mafias on the Move* analysing the poor adaptation of the Solnstevo group to Italy.[26]

6   Globalisation through Cyberspace

The most important element of the globalisation of Russian organised crime has been through cyberspace. The first large-scale manifestation of this was in the late 1990s when they became deeply involved in the dissemination of child pornography. But their technical expertise has helped make them major illicit actors on both the Internet and the dark web. They conduct illegal activities not only for their own personal grain but also provide services to other

---

[23] *Armenian Criminal Gang Dealt Serious Blow*, January 8, 2015, https://www.fbi.gov/news/stories/2015/january/armenian-criminal-enterprise-dealt-serious-blow/armenian-criminal-enterprise-dealt-serious-blow.

[24] Croft and Belton.

[25] Raymond Bonner, *F.B.I Going to Budapest to Hunt the Mob*, February 21, 2000, http://www.nytimes.com/2000/02/21/world/fbi-going-to-budapest-to-hunt-the-mob.html.

[26] Varese, *Mafias on the Move*.

criminal groups who need high level criminal tools that they do not have the expertise to manufacture. As one analyst of Russian cybercrime has commented, Russian criminals were the first to "offer crimeware to other criminals."[27]

Therefore, their criminal activities in cyberspace can be divided into two primary categories: cyber enable crime such as illicit trade in pharmaceuticals, sale of fraudulent documents and the commission of fraud. Yet they often an important range of services from such tangible products as fraudulent documents to computer-related commodities such as malware, but they are excel at the new forms of criminality that have been created by the online world such as selling malware, malicious anti-viral software, botnets, ransomware and providing the tools to conduct denial of service attacks.[28]

Investigations and arrests of some high-level cyber criminals reveal that they are not just youthful hackers but much more seasoned global actors who combine their knowledge of the cyberworld with an ability to set up offshore accounts and effective payment systems to be compensated for their criminal activity. A detailed analysis of a crime ring behind the largest distributor of spam on the Internet, revealed a sophisticated crime organisation that functioned across three continents –Asia, Europe and the US to market pharmaceuticals, primarily Viagra, to ready buyers. The group worked through banks in the former USSR that had correspondent banks in the US. This crime group had previously been in the marketing of child pornography and after their access to the financial system was cut off as a result of their pharmaceutical crime, they moved into other areas of computer crime such as fraudulent antiviral software.[29]

Russian organised crime has been deeply involved in the sale of stolen credit cards for at least fifteen years. Initially, the card information stolen on line were sold in open markets such as in Odessa in the early 2000s. But now both the theft and the sale goes on in cyberspace.

Europol has identified Russian-speaking groups as key actors of online card data thefts.[30] In the United States, a group has been identified in stealing the

---

27 Max Goncharov, *Russian Underground Revisited*, 2014, 4, http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf, Goncharov, malicious anti-viral software Russian Underground.

28 Ibid.

29 Brian Mccoy et al., *Pharmaleaks: Understanding the Business of Online Pharmaceutical Affiliate Programs*, www.usenix.org/conference/usenixsecurity12/technical-sessions/presentation/mccoy; Interview with McCoy; Krebs.

30 Europol, *The Internet Organised Crime Threat Assessment*, https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015, 38.

records of 83 million customers at JP Morgan Chase in 2014.[31] The scale of this activity and its global impact reveal the enormous reach of Russian organised crime in cyberspace.

7   Conclusion

Post-Soviet Russian organised crime has successfully globalised in both the real and the virtual world. This process of globalisation began in the final years of the Soviet Union and has become more pronounced in the following decades. The absence of political will and of law enforcement capacity to address the problem within Russia and other Soviet successor states has contributed significantly to its growth. On the domestic arena, almost no serious criminals or their facilitators have been prosecuted. The international community has had some success in pursuing the traditional Russian organised crime figures but much less success in pursuing the high-level networks that commit or facilitate transnational criminal activity, especially in the cyberworld. The very significant amounts of money being successfully laundered overseas illustrate the complicity of wilful blindness of many bankers, real estate agents and professionals who enable the movement of dirty capital abroad.

The high technical capacity of the criminals and their ability to operate in many jurisdictions simultaneously suggest that Russian-speaking organised crime will remain a significant challenge for the global community in the coming period. This will be especially true of Europe and the United States that remain rich targets of opportunity for these criminals.

---

[31]   Brian Krebs listserve, *Arrests in JP Morgan, eTrade, Scottrade Hacks*, November 10, 2015.

Combating Organised Crime – The Role of Eurojust

Benedikt Welfens

Eurojust The Hague

Eurojust was founded on 28 February 2002 based on the Eurojust Decision of the Council and started in the end of 2002 at The Hague after the premises were finalized. The creation of Eurojust had also been the result of the fact that on police level Europol had been stablished, also based in The Hague. The European Union (EU) Member States realized that in a world without borders (at least in the EU – at least until now) there was and is a need for a closer and better cooperation in the field of justice especially when it comes to organised crime and specifically to organised crime groups. The existing rules concerning cross border cooperation between judicial authorities in the EU are not offering enough and efficient tools in order to lead a successful fight against organised crime taking into account the limited budgets in the EU. As a result of the decreasing budgets, the Member States are not always able to completely adhere to the agreements they have signed. Bearing in mind that the EU consists of at least 28 different judicial systems (reflecting the song of U2 "One" with the well-known line: "we are one but we are not same") which are working quite well inside the countries where these systems are used but as soon as we realize that crimes do not stay inside the national borders it is quite obvious that the mutual legal assistance becomes really difficult due to the variety of the different legal systems. But mutual legal assistance is the key to any effective cross border investigation in the EU and also with Third States outside the European Union.

Let us have a closer look at the mutual legal assistance instruments/agreements and how these are used it became obvious that there was a need for creating Eurojust. Normal mutual legal assistance is quite slow, the answers of the requested Member States often come very late, if they come at all, the quality of the translations of thousands of letters of request (LoR) is often poor and not always understandable and as a result of only partly answered LoRs. New LoRs will be sent out and the same unsatisfying procedure starts again. This delays an enormous number of investigations, leaving all parties involved frustrated. Furthermore, in many cases it will be too late to confiscate the profits of the crimes committed when the answers to the LoRs finally arrive. This also might lead to lower penalties for the perpetrators due to the long time a given investigation needed to come to an end with a final verdict. The former extradition rules in the EU and the later created European Arrest

Warrant (EAW) show in an impressive way how a closer European approach might be very successful and feasible in all EU Member States. The average time to extradite a person from one EU Member State to another decreased from more than one year too just more than one month after the EAW had been established. All Member States realized that there is a need to coordinate cross border investigation in a better way.

Having said this and keeping in mind the wonderful idea of creating an "area of freedom security and justice", the creation of Eurojust was a necessity in the fight against organised crime. At Eurojust you will find 28 EU Member States represented by their national desks in the permanently based premises in The Hague. The representatives are always experienced prosecutors and judges, and occasionally police officers as well. They have an excellent network with regard to their home authorities and a very good knowledge of their national judicial system. The official language at Eurojust is English, so there are no problems at all concerning the communication between the EU Member States. The national desks are able to provide a kind of guarantee for clarity, speed and certainty in MLA issues. Eurojust also has legal personality resources and equipment for coordination meetings and conferences. During coordination meetings Eurojust is offering interpreters so that all authorities involved in a cross border case can contribute in the best possible way and misunderstandings are being avoided. Eurojust is covering the costs for two persons per country, which means that very often a prosecutor or an investigative judge plus a police officer will join the coordination meeting. Of course more practitioners who are working on a case are welcome but the further costs have to be borne by the country which wishes to send more than two people to join the meeting.

Europol, OLAF and other European agencies are very often involved and are able to deliver another added value with their specific case analysis and additional information! This also enhances the cooperation between judicial and police authorities which is crucial for any success in the fight against organised crime taking into account that in all EU Member States the budgets of police and justice are often reduced to a point where one might doubt about the political will in the fight against crime in general. Eurojust and the national desk which is organizing the meeting are offering advice and expertise without interfering in the investigations. As a result of nearly every coordination meeting, an acceleration of all ongoing investigations can be observed, a better motivation of everybody involved (similar problems in all EU Member States) – very often all authorities agree on a common action day where simultaneously suspected persons will be arrested, premises will be searched and illegal profits will be confiscated in all involved countries.

Eurojust provides a specific secretariat to support the creation of joint investigation teams (JIT) by offering advice based on the creation of JITs at Eurojust in more than hundreds of cases. Additionally this secretariat can provide funding up to 50,000 Euros for the JITs, covering costs that arise from for example translation, traveling and accommodation. When needed also costs for technical equipment like laptops, mobiles etc. can be refunded. Since the usually slow channel for demanding information via a LoR is exchanged by direct contacts between the partners of a JIT the creation of a JIT always speeds up the investigations in all countries involved. And finally Eurojust created the so-called coordination centre. What does that mean? During a coordination meeting at Eurojust in The Hague or in another country (if appropriate and not more expensive than a meeting at Eurojust in The Hague) the involved countries very often agree on a common action day in the involved countries (see above). On the action day there will be one person from the National Desks involved observing the action in real time in a conference room and they are always informed about the progress of the execution of measures by their home countries. If additional action suddenly has to be taken, the information flow can be handled immediately via the members of the coordination centre who forward this information to their home authorities outside of Eurojust. The fact that Eurojust is working on a high level and is accepted and appreciated more and more finds its reflection in the statistics of Eurojust. The case numbers have increased continuously since Eurojust was established:

Figure 1. Casework Statistics, 1 January – 31 December 2013.
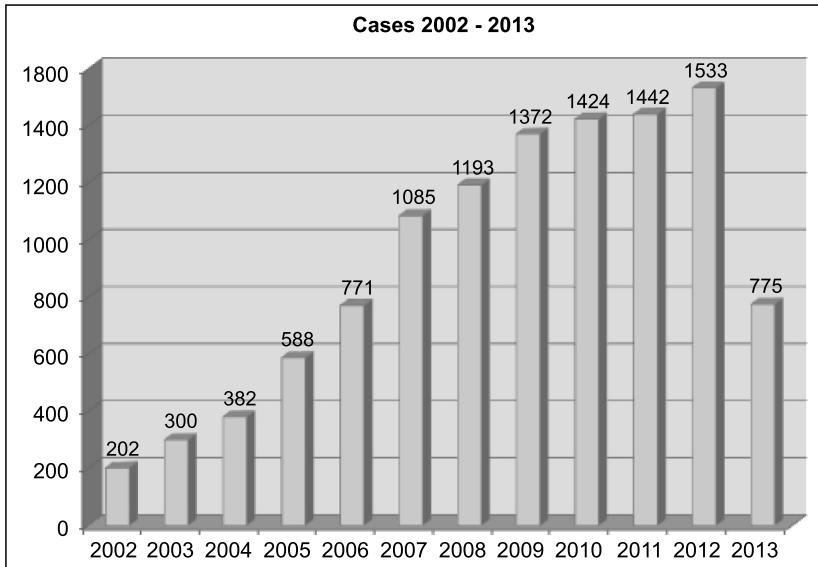
This year Eurojust will reach the number of 2000 cases. Especially the German Desk is increasingly involved in supporting German authorities in cross border investigation and supporting colleagues from other EU member states. This fact also demonstrates the mutual trust between practitioners in the EU when it comes to real criminal investigation where we need each other no matter how different the judicial systems in the involved countries are. It also proves that the idea of a closer and better EUROPE does work out when it comes to practitioners on police or judicial level.

Here a simple example of the work Eurojust is delivering since 2002:

The prosecution office in Reggio Calabria requested the assistance of Eurojust in a case concerning the smuggling of a massive amount of cocaine from South America to Europe. A coordination meeting took place at Eurojust where all relevant information was exchanged and where it was agreed to establish direct contacts between Germany, the Netherlands and Italy. Wiretapping took place in the countries involved, the information gathered was exchanged in real time and as a result of this cooperation it was finally possible not only to detain in Calabria a ship from Venezuela bound for Rotterdam with one ton of cocaine which was confiscated but also to arrest several dan-

gerous suspects who were members of the "'Ndrangheta association" and had been fugitive for several years. Without the close cooperation started at Eurojust during the coordination meeting including the precious work of the interpreters, the normal way of exchanging information, letters of request which due to a limited quality of translation might be occasionally misleading and difficult to answer, the acceleration of all investigation measures and the resulting success would not have been possible at all. After a coordination meeting is before a coordination meeting – giving a positive example it offers not only more motivation for the involved parties but very often is also the basis for a better cooperation in the future going back to the contacts established between the practitioners during a coordination meeting.

To use Eurojust – if needed – to use Europol – if needed – as a tool to improve cross border investigation is always a safe and good investment in the fight against organised crime bringing us forward step by step to a better and more secure Europe.

Metal Thefts and Mobile Crime Groups in Sweden

Johan Lundberg

Swedish Police Authority, Gothenburg

Metal theft as such refers to "incidents in which items are stolen for the value of their constituent metals" (Sidebottom 2012) and notably, this crime field involves a lot of variation within the respective categories of metal theft. Moreover, as the prices of many metals have increased over the past years, it is difficult to estimate the volume of metal theft (Sidebottom 2012). Furthermore, in the example of metal theft, one can observe how changes within society can evoke opportunities for crime (Sidebottom 2012), as the increasing price and value of metal makes this crime field very attractive for criminals. As will be also made visible in the following, metal theft is largely carried out in areas with low surveillance such as railroads, construction sites and churches as it reduces the risk of being detected (Sidebottom 2012). According to Sidebottom, there are two types of offenders: "smaller" thieves, who steal easily removable items, and more organised groups, who are also involved in trade and steal on a larger scale (2012). As metal theft is also referred to as "one of the fastest growing crime types internationally" (Sidebottom 2012), it is of even greater importance to develop measures to curtail this uprising crime field. Therefore, the presentation merely concerned two special operations that were approached within the Police Region West in Sweden. The first operation is connected to metal theft and the second operation is connected to crimes against elderly people.

1 Operation "Coppersnake"

Before operation "Coppersnake" started, the scale of metal theft was unknown by the Swedish police and other authorities. When analysing the crimes related to metal theft, the magnitude of the crimes soon became clear. Among other evidence, the police found 60 stolen trucks in the surrounding of Gothenburg which carried metals with an estimated value of 100,000 Euros. The operation came into light in 2006, when the Police District of Örebro confirmed that metal thefts had become an increasing problem in the area. The police authority of Västra Götaland made a general investigation of the metal thefts which resulted in a report. Based on this report, the police authority initiated "Operation Kopparorm" in December 2006. The name of the operation is originated in the connection between the metal thefts and copper

which was mostly stolen. The analysis of the metal thefts established that companies in Gothenburg bought stolen metal from thefts all around the country. Moreover, none or only inadequate identification of the sellers could be detected as there were no receipts and it was only paid in cash. The thieves handled their stolen goods via tax evasion, which of course decreases the risk of being identified. Furthermore, it can be concluded that churches and cultural buildings are affected as well as power companies and the Swedish railroads. With regard to churches, for instance, copper downspouts and copper roofs were stolen. From the railway, these criminals steal the steel earth wire which is made of copper; this of course poses a sharp disturbance in train traffic and threatens the infrastructure. Another finding concluded that the metal companies, which purchase metal in the value of 15 million Euros each year, paid no taxes. In this business alone, the companies withdrew approximately 50,000 Euros in cash every day which costs the state about 100 million Euros each year. At this time we found long queues outside metal companies in the early morning with thieves who have been out and steeling in the night and wanted to receive their payment in cash. After receiving the stolen metal from the thieves, the metal companies take the metal and produce copper in granulated form. After the granules have been produced, it is very difficult to trace the metal parts. As a result, the analysis revealed that metal thefts are a public danger as well as a threat to the infrastructure.

1.1 Proposals and Measures

We immediately started to cooperate with other authorities and drew representatives to the meetings which were led by the police. The authorities who were invited to the meetings were: tax authority, enforcement service, and the city of Gothenburg, customs, eco-crime authority, Social Insurance, insurance companies and branch organisations. The closest cooperation in these cases was led with aid of tax authorities. The measures taken start with the police visiting different metal companies to gather information about the business. Thus, they have increased the surveillance and the control over the businesses in order to interfere with pressure. Crime prevention also marked an enormous pillar within the cooperation with the authorities, as it was detected that the companies where the stolen goods come from stored the copper outside the company which facilitated the search for the copper. Moreover, legislative amendments were proposed: scrap dealer permissions were reinstated and it was prohibited to use cash. Another important legislative measure includes DNA science. The developed system named DNAnet is used to avert thefts of copper wire or other copper-related items in the national railroad system. It is used as "evidence marking" and is applied directly to the metal and can there-

fore be traced back to a specific crime[1]. At the same time, the tax agency conducts audits on the current conduct which is a very effective method to disturb and control the business. After the audits are carried out, the police checks and disrupts the business at companies. Furthermore, meetings with industry representatives are scheduled and the municipality conducts oversight of the environment. An example was mentioned in which the social insurance authority had to deal with a case against a metal dealer who sold the metals for 9.7 million Swedish krona and at the same time received compensation. In addition, when we surveyed the merchants, 65 rogue metal dealers were discovered in the region.

1.2   Results Thieves and Results Scrap Dealers

The leading group consisted of people from former Yugoslavia and the main active members were in general of Romanian origin. The police was led to believe that the Romanians were used as slaves, as they were poorly paid and the majority of their income had to be given to the head of the group. In conclusion, the persons steeling did not make vast profit in parity with the main actors. As a result, the people involved were sentenced to 25 years in prison in total; the criminals caused damage with the thefts they carried out in a value of 2.5 million Euros at least. Those thefts include crimes such as tax crimes and can be summarised under the term of organised crime.

Regarding the scrap dealers, nine were convicted in 2011 for tax and accounting offences. In total, the key player within the scrap dealer groups had to serve 13 years in prison and caused damage in a value of 10 million Euros. As these offences mostly included tax fraud, the criminals also caused large debts within the Swedish Enforcement Authority.

1.3   Key factors for Success

Among the key factors for success which have been proven throughout the aforementioned measures and proposals are: a national focus, one group with a national responsibility is effective, a prosecutor assigned to the group, all trials are approached in one court, cooperation with other authorities, resources for investigation, the need for intelligence personnel with full time focus on metal thefts and the importance of persistence as the investigations last a long time.

---

[1]   For more information on the release details approach: http://www.adnas.com/SMPR/applied-dna-sciences-DNAnet-system-protect-copper-theft-sweden.

Today, three years after the operations, it is the first time that legislative laws regarding metal business are changing, for it is now prohibited to use cash payment. In fact, the measures which have been taken enhanced the decrease of metal theft in Sweden. However, it is noteworthy that the reverse charge only applies to the trade between businesses; this was in charge in 2013/14. Only sales of waste and scrap metal are covered by the rules of reversed charge, since it is always the buyer who must report and pay the Value Added Tax (VAT). Sweden is also overseeing the legislation regarding the authorisation to run metal trade companies. Another interesting point could be seen in an article in the *Washington Times* from November 2013, which describes that the US, specifically the Senate Judiciary Committee is ready to take action on a bill that would make metal thefts a federal crime and carries a ten year prison sentence for anyone convicted of stealing metal from highway equipment, telephone or cell towers and other critical infrastructure.[2]

2 The CIRCA Unit

The unit started in 2009, is located in Gothenburg and Vårgårda and consists of ten employees who are occupied in the fields of desk, investigation, analysis and prosecution. A central pillar within the Central Investigation Related to Criminal Aliens (CIRCA) unit involves a distinct investigative and international perspective.

2.1 Perpetrators

The perpetrators are members of Mobile Organised Crime Groups (MOCG's) and are often of Romanian and Bulgarian descent. They are known for several offences around Europe.

2.2 Offences

Offences which were detected included shoulder surfing[3], theft by distraction, pick pocketing and robberies.

---

[2] Link to the article, published in the "Washington Times", June 11, 2013: http://www.washingtontimes.com/news/2013/jun/11/senate-moving-make-copper-theft-federal-crime/.

[3] This term refers to direct observation techniques to garner passwords, PINs, security data etc. and is conducted through observing the input combination from e.g. cash dispensers to accordingly use the data to illegally enter the bank account or collect sensitive data. From http://www.itwissen.info/definition/lexikon/shoulder-surfing.html.

2.3   Figures

In average, the Swedish police convicted ten MOCG's per year that were firstly travelling around Europe and later on were arrested by the Swedish police.

In average, a MOCG consists of two to four persons, whereas each MOCG can be linked to about 20–30 offences. Each member of a MOCG is usually sentenced to two to three years in prison. More notably, they profit from every theft in a value of approximately 1,000–1,500 Euros per theft. Furthermore, close to half of the MOCG's identified are from Romania. They are known for several offences around Europe and in some cases not known in their home countries for their on-going criminal activities, despite they have a criminal record. In many cases they are not at all known by the police in their home countries.

3   Questions for Discussion

In closing, there are still some question open to discussion in order to fully get a hold of the constantly increasing metal theft problem. How do we break the anonymity of the MOCG, both abroad and in their home countries? More importantly, how can we prevent the crimes? In which ways can we prevent the recruitment of new members to the MOCG? How can we create "early warnings"? One approach to this question might include the placement of informants inside the MOCG in order to attain intel into the procedure and structure of MOCG's.

Furthermore, the key factors for success already mentioned could provide support for solving some of the previous questions. With regard to creating early warnings as well as the prevention of crimes, international cooperation plays a key role, despite the already existing cooperation could be extended. With reference to intelligence, Europol is also a very important partner in combatting Swedish metal thefts. Among other factors which cannot be stressed enough, persistence with the investigation and a holistic perspective are perceived to be essential for deterring this specific crime field.

Bibliography

Sidebottom, A. (2012). Metal theft. JDiBrief Series. London: UCL Jill Dando Institute of Security and Crime Science. ISSN: 2050-4853. Available from www.jdibrief.com.

The local Dimension in the Containment of International Organised Crime: the Dutch Example

Cyrille Fijnaut

Tilburg University

1 Organised Crime: A Questionable Definition

1.1 The History of the Problem

In Europe the concept of OC is politically as well as scientifically acknowledged due to a political framework which can be observed in the passing of ad hoc laws targeting OC (Fijnaut/Paoli 2004: 21). Scientifically it has become a topic of interest in the fields of social sciences and criminology. Moreover, OC is now a synonym for illegal enterprises which focus on gaining profits through illegal activities (Fijnaut/Paoli 2004: 28).

Looking at the current OC situation, these bandits are crossing borders, including those of Sweden, the Netherlands, France and Germany which is not a new circumstance. Rather, banditry is perceived to be a historical and an au courant phenomenon as Dutch historians, including Florike Egmond, wrote about bandits operating from Paris to the North of the Netherlands and to Mainz. Large criminal networks engaging from all over Western Europe can therefore easily be compared to one another as they do have a lot of characteristics in common.

The same accounts for the urban underworld: For example, there was reference made to Amsterdam. Books on the history of the city described how up to the 1960s, the underworld of Amsterdam was a "cosy corner" since everyone knew each other. When walking around the heart of the city of Amsterdam today or walking from the central station up to the South of the inner city, it is like a cosmopolitan centre – the global village on just a few squares of kilometres. In conclusion, the "cosy corners" and the population have changed a lot, but nevertheless, it is to some extent still the same place. As a result, the urban underworld developed from marginal pockets to cosmopolitan areas.

Hinting at one of the most widely used words during the conference, namely "international", there was reference made to the discussion at the end of the 19th century on the "international criminal" in the field of criminology and criminal law. Due to the urbanisation in Europe, the increasing railway sys-

tem and the car industry flourishing, the international criminal was on the agenda of a vast discussion. In German and French criminological journals the international criminal was a common described subject which is the reason why common identification systems to identify criminals across borders were established.

What does international mean then? As there has been familiarity with cross-border crime problems for a long time now, these systems are not an invention of the United Nations (UN), nor have they sprung from a genius mind. The context and history of the problem can therefore be divided into three main facts: Firstly, banditry as a historical and contemporary phenomenon, secondly the development of urban underworlds from marginal, small areas to cosmopolitan areas and lastly the international criminal as an old concept and living reality in Europe. As OC mainly exists because there are people who actually demand the illicit goods which are provided by organised criminals, this invokes a negative side-effect: OC refers to people involved and also to activities carried out (Fijnaut/Paoli 2004: 29). Accordingly, the next two chapters are focused on these origins of the OC problem.

1.2 The Nature of the Problem: Activities

The next topic includes the nature of the problem with reference to a first piece of comparative research on a comparison between the United States and Western Europe (cf. Fijnaut). It was concluded that there is a lot in common when it comes to defining OC as delivering goods and services on black markets. This is exactly what corresponds closely to the reality in Paris, London, Amsterdam, Chicago and New York, whether it is the trafficking of arms, drugs or humans: The difference is close to zero. Although, there are differences with regard to the illegal control of legitimate markets: the ways in which the Cosa Nostra controlled the waste industries in New York, for instance, or social housing and food markets in the past, tell a different story. To note, in the history of various EU countries it is apparent that similar crime structures occurred, whereas the term "OC" was seldom used. Despite this, as OC also developed with time, modern OC has different faces now than in the 1960s (Fijnaut/Paoli 2004: 21).

There continued to be an examination of the situation in the inner city of Amsterdam and people asked what we are talking about exactly. Are we talking about criminal groups organising black markets? Are we talking to some extent about the usage of the usual legitimate world and order embedding their illegal activities to gain the most profit or are we talking about criminal groups which try to control legitimate markets in Amsterdam? It was then clarified that one has to have a specific understanding of what OC actually

means in an urban environment in order to understand the problem in such a peculiar situation. Thus, the main categories of problems in OC with regard to activities are serving black markets and controlling legitimate industries. The distinctions of OC in various countries, with respect to white collar crime and terrorism for instance, are decreasing. Nevertheless, there are quite important overlaps when it comes to professional crime and street crime.

1.3   The Nature of the Problem: People

When it comes to the problem not just in terms of activities, but in terms of people, OC is quite an arduous topic when looking at the inner city of Amsterdam. Are we just focussing on the Hungarian human traffickers trying to recruit women from Bulgaria or Romania and transport them over night from Budapest to Amsterdam? Or should we also look at the people who aid and facilitate such structures for OC? With reference to the example of transporting women to Amsterdam, it was stated that one would have to look at the hotels and the people who rent the windows for prostitution and claim to know nothing about human trafficking. How far does the OC problem really go? A central claim includes the call for targeting the supporters of OC as well as the profiteers of OC.

This was further illustrated by an example which was covered by the media: Hans Zondervan sued Philips for no longer supplying him with light bulbs and switches he used for the cultivation of cannabis and also sold to various other cultivators. He further claims that Philips continues to cooperate with the cannabis industry and demands compensation for his lost revenues[1]. It was then mentioned that Philips has made a lot of profit from the illegal cannabis cultivation in the Netherlands. And the moment the story went public, Philips tried to stop the selling of their lamps to the illegal cultivation. So should Philips also be targeted and prevented from selling those lamps, as they are embedding and enhancing the illegal cultivation of cannabis in the country? Subsequently, OC is not only structured in chains and networks, but also in junctions and the people connected to these junctions are not only organised criminals, but also supporters and profiteers of OC.

As the example clearly illustrates, not only criminals but legal companies are equally – willingly or unwillingly – involved and profit from OC and in this way support organised criminal activities and therefore further the spread of the OC problem.

---

[1]   Cf. to the following article in *Dutch News.nl* in May 2015: http://www.dutchnews.nl/news/archives/2015/05/philips-faces-legal-action-over-light-bulbs-for-marijuana-plantations, accessed on 26th October 2015.

1.4   The Context of the Problem

There are various aspects within the context of the problem such as the local/ national and transnational dimension. The meeting in 2000 in Naples where the UN convention on transnational OC[2] was signed, the question to what the term "transnational" actually refers to was also raised. Looking at the inner city of Amsterdam it was asserted that to some extent, there is nothing transnational about OC because it stays in the inner city. When visiting the task forces in New York, they recounted their experiences with OC which also were solely accounting for New York. In particular, the five mafia families in the city were not controlling legitimate markets in the Netherlands or in Germany; hence this was rather a local problem in New York. What does transnational refer to then?

In the following, the political reason to define OC as a transnational phenomenon illustrated: During the convention it was said that this adjective should be used to prevent people from thinking that specific countries as the main source of OC, as e.g. Italy, China or Colombia, were targeted. The term "transnational" should neutralize the implication of OC, but it also estranged the countries from their responsibility for OC.

In 1992/1993, the involvement in a committee of inquiry in the Belgium parliament occupied with the trafficking of women in which Belgian pimps recruited women from the slums of Manila and brought them to Cyprus, to Italy, Brussels etc. and then put them into carousels, was given account for. To some extent, it is transnational as they had to transport these women from the slums of Manila to Amsterdam airport, thus a good level of communication was needed. Also, these criminals had to pay the people in Manila who recruited the women and accordingly also used the international banking system to pay for this service.

Nevertheless, it was claimed that in the core, it is still a national problem and requires local effort: if you want to stop the trafficking of women from the Philippines, everything should be done to prevent the fact that women can be recruited in the slums of Manila. Furthermore, the countries the women were exploited in pose no transnational phenomenon because this exploitation is not invisible and happened in various cities in The Netherlands, Belgian, Germany etc. If people want to do something about human trafficking, they have to realize that it is not just a transnational problem, since one would then never be able to contain it. If the local authorities are not able to curtail the

---

2   For further information on the UN convention(s) please account: https://www.unodc.org/un-odc/treaties/CTOC.

problem, the problem will never be contained. Therefore, the local dimension of OC is gargantuan in many ways.

Take for instance the Netherlands: The main criminal problem in the Netherlands is the illegal cultivation of cannabis and the production of synthetic drugs which already started in the 1960s to serve the markets in Sweden. Despite, the cultivation of cannabis is to a large extent a local problem which takes place right in the neighbourhoods of Tilburg and other cities and in villages as well. The same accounts for the production of synthetic drugs. It was indicated that the Netherlands have developed into the Colombia of synthetic drugs and cannabis. And it may be clear that the Netherlands itself has to counter these problems because one cannot expect an involvement of Italy or France to do this.

Examining the aforementioned points with regard to the context of the problem, the local/national as well as the transnational dimension, the globalization of the infrastructure, the urbanization of mankind and the role of (civil) war, dictatorship and failed states all have to be accounted for in order to reach to the core of the problem.

1.5   The Containment of the Problem

Until the 1990s, OC was very much ignored on the political agenda although serious crime enormously increased in the previous decades due to the emergence of drug trade (Kleemans 2004: 303). A vast amount of time passed before authorities realized they had a problem. But not only in politics, but also in the academic field, OC was considered as a "foreign phenomenon" (Kleemans 2004: 303) and basically no empirical research existed. In 1992, the OC problem was on the political agenda and considered as a major threat which resulted in a preventive and repressive approach and in the establishment of squads in order to counter OC (Kleemans 2004: 304).Thus, the local dimension in the OC problem demands very decisive measures to solve the problem in its roots.

What is important for the Amsterdam situation is that if one wants to contain this problem to some extent, criminal law is indispensable. Especially with regard to the American police authorities'[3] successes in combatting e.g. the La Cosa Nostra families in New York[4], it was reassured that when confronted with such organisations, criminal law, heavily organised and armed, is inevi-

---

[3]   Here referring to the FBI and the NYPD.

[4]   For further information on the case consult the "mafia commission trial": https://en.wikipedia.org/wiki/Rudy_Giuliani#Mafia_Commission_trial.

table. Firm support of criminal law in this area was remarked, not only to convict people, but also to specify the problems as criminal law and criminal justice are excellent mechanisms to illuminate an issue. Accordingly, people from the "outside world" are also informed about the situation as the police have tested evidence and judges have to agree upon it to bring forward a case.

Furthermore, criminal law is important because it supports administrative measures against OC groups. When Rudolph Giuliani became mayor in New York, he used the insight and knowledge of the related task force members to deal with the illegal control on legitimate markets. In the beginning of the 1990s, members of the task forces moved to the inspections in the town hall in Manhattan and started to clean up the mafia controlled businesses.

As an example, the waste disposal in Manhattan was cited: The five mafia families obtained a monopoly on waste disposal in Manhattan and made a lot of profit from it because they did not accept any competitors. Giuliani withdrew all the companies' licenses overnight and forced them to reveal their identity if they wanted to continue with their business. As a result, there is a very lengthy form which has to be filled out and which identifies the person as well as the origin of the money and social security number. If the form is filled out with false information, the person will be banned from the licensing process. This is a great example for illustrating the way in which knowledge and information, gathered by the in-depth application of criminal law, was used for administrative purposes in order to clean the legitimate markets.

This approach also poses an important pillar of the policy in the Netherlands. Criminal law is important dealing with organised crime problems, but it has to be embedded in a broad range of measures to contain OC. The aforementioned example of course is touches upon the local level of OC because not everybody can issue licenses. This does not mean, however, that international conventions on mutual assistance or institutions like Europol or Eurojust are not important. On the contrary, it was affirmed that e.g. Europol, which is functioning as a hub for intelligence information about mobile OC groups is in a complementary sense quite important, but cannot take over. These institutions do not dispose of "real" powers, but are rather supporting, coordinating and overarching, although it may be said that they are moving into a more operational role. The real powers are still located in national and local authorities, as they are in charge with regard to criminal law and administrative policies.

As a result, the following points are worth considering for the containment of OC: the role of criminal law and the criminal justice system, the necessity of an administrative and fiscal approach, the importance of strong local/national policies and authorities, the relevance of international conventions on infor-

mation exchange and mutual assistance in (criminal) matters and the complementary role of European/international institutions.

2 Organised Crime in the Netherlands

2.1 A General Picture of the Scene

Examining an overview of OC in the Netherlands, the focus lay inter alia on OC in the field of black markets with regard to the cultivation of cannabis on a vast scale. Estimates say that 75 to 80% are produced for the export and the remaining 20% are produced for domestic use. Moreover, the production of synthetic drugs forms a massive problem within the Netherlands. To further illustrate the extent of the problems, another example was consulted: a few years ago in Tilburg, just five kilometres from the Belgian border, a task force was established which came into contact with a crown witness willing to talk about what was really happening in the neighbourhood. They came to the conclusion that in Tilburg city, a city of more or less 200,000 inhabitants, ca. 3,000 people are involved in the illegal cultivation of cannabis. Thus, only accounting for the city of Tilburg, there is an estimated sum of money of about 700 up to 800 million Euros circulating in that business. Furthermore, it can be noted that the Netherlands are at the cross-roads of incoming and outgoing international criminal networks, trading in hard drugs, women, small arms etc.

2.2 The Hard Core of the Problem

The question therefore remains on where the money of literally millionaires in illegal business is invested in. Is it invested in real estate? Will it be invested in illegal companies? Will it be used to corrupt public officials? The present situation in the Netherlands is completely contradictory to the self-image of the Dutch which consist of a "high level of social stability and a certain degree of tolerance" (Van de Bunt 2007) especially in the South where the situation seems to be the most pervasive: mayors are threatened and intimidated and officials are threatened at the town hall, as they want to protect the Dutch interests.

The Dutch government already established a system of screening years ago following the example of New York: screening applicants for licenses and screening people for the bidding process. There has been established a national bureau within the framework of the Ministry of Security and Justice which has access to all data in the Netherlands like data from police, judiciary and tax authorities. If local authorities are of the opinion that an application is

suspicious, they can request advice from this national bureau which collects the information at hand and gives advice to the local authorities that there is perhaps a serious risk of abuse of such a license, hence the license will not be issued or will be withdrawn.

Accordingly, the first lines of defence against organised crime are no longer the prosecutors, but rather the mayors due to the administrative approach to OC problems. Thus, their important position in combatting the OC problems puts them in the sights of criminals who start attacking and intimidating the mayors. If these mayors were powerless, why would anyone attack them?

It is similar in the case of corruption: why would one corrupt authority when they stay passive and do not try to contain the OC problem? Only the moment that these officials become active and threaten the criminals' interest does it makes sense to corrupt them. So the only other way to influence powerful authorities is to intimidate them if they are not corrupt. Fortunately, the Netherlands has an integral local authority system, so corruption is not so much the problem, but due to their integrity, the local authorities become the victims of intimidation.

Summing up, the hard core of the problem consists of the production and exportation of drugs, the trade in hard(er) drugs, arms smuggling, human trafficking, the predominant role of Dutch criminal groupings, the growth of illegal economies and parallel societies and the investment of criminal profits in i.a. real estate.

2.3 The Fierce Debate on the "Legalization" of Cannabis (and Synthetic Drugs)

Currently, there is a fierce debate on the legalization of cannabis, but why is it a fierce debate? It is fierce for a number of reasons: when dealing with huge black markets and large scale illegal production of cannabis and synthetic drugs, the main issue raised in this debate is whether this whole process should be legalized in order to get a hold on this problem. Furthermore, it is claimed that when putting the label of crime on the cultivation of cannabis, the Netherlands are to some extent organising the black markets themselves. When these markets develop, there are always people who can make profits from them and who deliver and serve these markets, thus the idea is that legalization, as probably the most effective structural strategy, would prevent this development from happening.

Nevertheless, as can easily be imagined, this is quite a controversial issue to try to cope with OC by legalizing/whitewashing these black markets. To some extent it actually is coherent: looking at the history of gambling, one

can see that a vast amount of research was done. In the United States, for instance, the only state where gambling was not illegal, where one could receive a license, was Nevada. In the other states gambling was illegal and this created massive black markets. When taking into account the US reports on OC in the 1960s, the police corruption problems in New York can be straight forwardly linked to illegal gambling. Therefore, the discussion whether gambling should be legalized in the US was reinforced. Not only could the state increase its profits and make more money from this illegal market, but it was also an opportunity to deal with the corruption and OC problem. In conclusion, one could state that the legalization process of gambling is a wise strategy because now looking at the US, the states and even the Indian reservations are fighting for a casino as a lot of money can be extracted from gambling.

Referring back to the legalization of cannabis, it is also stated that e.g. Colorado and Washington State already have legalized the cultivation of cannabis and the results for Colorado show that during the first year of legalization, a profit of ca. 600 million dollars was gained from the newly legalized market. Furthermore, the US supporters of the legalization of cannabis also take the view that this is the only way to deal with OC problems.

Furthermore, it was outlined that a number of people in the Netherlands defend the thesis that the government should also dare to take the step of legalizing the cultivation of cannabis. The Netherlands or Belgium cannot take this step on their own, however. Rather, the process of legalization should occur in the framework of the European Union (EU) with a common position defined which could then be defended on the level of the United Nations (UN). Maybe Germany could also join this framework, as a female politician in Berlin recently requested permission to open up a coffee shop and the Federal Institute for Drugs and Medical Devices (BfArM) stated that they did not have jurisdiction to issue a license. Thus, they avoided the burning question regarding the legalization of cannabis. Moreover, it would be important to overcome traditional notions of crime and black markets in this field, nevertheless, as already has been stated; this cannot be approached on a national basis.

Summing up, whitewashing black markets e.g. with reference to the example of gambling, can to some extent be a very worthwhile and effective long-term strategy vis-à-vis OC problems in any case in that market. Of course the legalization of cannabis would not pose the end of OC, as they will shift their focus to other sectors, but in this specific sector it could make an enormous impact. In summary, the fierce debate on legalization in the Netherlands is grounded in the problem of coffee shops and cannabis cultivation. The arguments in this debate of both, opponents and supporters, form a political deadlock which raises the need for a "solution" for the EU.

3 The (Containment of) Organised Crime Problems in Amsterdam's City Centre

3.1 The Developments in the Years 1996–2006

3.1.1 The Efforts of the Local Authorities

The focus correspondingly shifted from the Netherlands in general to the centrepiece of the talk: the situation in Amsterdam. For a better understanding of the situation in Amsterdam, it is necessary to look further back in time: there was reference made to a book on the experience, context and outcome of a huge project between 2007 and 2011 in order to deal with serious OC problems in the inner city of Amsterdam. This project did not start in 2007, but rather in 1994 when the Dutch criminal justice system ended up in a crisis about the use of "pro-active" investigative methods of the Amsterdam-Utrecht Inter-regional Investigation squad (IRT) which accordingly had been dismantled. The main issue concerned the fact that IRT detectives, in order to catch high-level criminals in drug trafficking, wanted to increase the importance of informants in furtherance of a more reliable position within these networks. Tons of drugs were imported under the surveillance of Dutch authorities as they hoped that through building up trust, some informants would rise the ranks within the criminal networks (Kleemans 2004: 304).

This, of course, was considered an unacceptable method, even in the Netherlands, without any legal basis at all. Another issue concerned the integrity of the government due to the uncontrollability of the situation (Kleemans 2004: 304). As a result, this practice resulted in a clash between the police chiefs in the Western part of the Netherlands and the prosecution service and ended up in a committee of inquiry in the second chamber of the Netherlands during 1995–1996 which evaluated the criminal investigation methods used so far.

This inquiry gained the insight that adequate investigation methods were mostly not enshrined in the Code of Criminal Procedure and the organization of the police and justice system was not fit for this express purpose (Kleemans 2004: 304), which led to a number of reforms. The chair of the committee of inquiry also raised the question of what actually made up the OC problem in the Netherlands. What are the powers and methods in need of to deal with these problems? It was a the time quite difficult to answer these questions because the narrative on OC predominantly consisted of stories and anecdotes besides articles of journalists and the real problem of OC was not clearly identified, for an overview of this problem was not available. Hence, the situation was quite uncomfortable: there was an urgent need to define powers and methods to counter OC without really knowing the extent of the problem itself.

What in particular was discussed from the beginning was the usage of "penti-ti". This discussion indeed evoked the idea that OC in the Netherlands was similar to the problem of the Italian mafia, controlling legitimate markets and corrupting local authorities, and was rejected for this reason. On the other hand, after the analysis on OC, it was realized that there is the need to reward people to some extent for their willingness to cooperate with the police and judicial authorities. "Deals with criminals" were accordingly accepted in the conclusions of the final report if this method got regulated within a legal framework, but not the usage of crown witnesses. This distinction was made on the basis of the assessment of the OC problem in the Netherlands with regard to the seriousness of the issue as well as the measures needed to counter it in a fair, effective manner.

3.1.2 The National Impact of "Amsterdam"

In the framework of the research for the Committee of Inquiry is was underlined that at any rate the OC problems in the city centre of Amsterdam should be examined: If there exists a serious OC problem, not only serving and operating on black markets, but also infiltrating legal economies – the reasoning was – then it would be in Amsterdam. In order to explore the nature and seriousness of OC in Amsterdam, Fijnaut and two other members of the research group Fijnaut – Frank Bovenkerk tried to identify the "intertwining" between OC and the legal economy (Kleemans 2004: 305). About half a year was spent in Amsterdam in order to collect information with help of the police, the Prosecution Service, tax authorities, the Chamber of Commerce and branch organisations. The final shocking conclusion for the town council stated that there were 16 to 17 criminal groups who hold – so to speak – in some respects more power in the city centre than the local authorities themselves. It showed networks involved in OC and the prevalence of immigrant groups specifically in drug trafficking as well as certain criminal groups investing in real estate, predominantly in the red light district in Amsterdam (Kleemans 2004: 305). The power of these groups is thus originated in window prostitution, drug problems, all sorts of crimes related to night business as well as real estate, which enabled these criminals to increase their influence. Correspondingly, it was defined that no criminal syndicate was detected and there was no control over the legitimate sectors of economy, which clearly differs from Italy (Kleemans 2004: 305). Nevertheless, there was a clear threat that the city centre of Amsterdam was moving into a dangerous situation.

When presenting the results to the town council, they accepted the definition of the problem. The next question raised concerned the methods and measures which should be taken to combat OC. The solution was found to be a differentiated strategy. Firstly, control over real estate in the city centre had to

be regained, since infrastructure is very important when it comes to apparent black markets. After ten to fifteen years, Amsterdam, or in any case bona fide institutions and businesses, used special funds to purchase more than 100 crucial buildings in the city centre. Secondly, another strategy included screening the applicants for e.g. licenses which resulted in the establishment of a special bureau in the town hall with great access to data and information. This bureau gave the mayor advice with regard to the issue and the withdrawal of permits, hence cleaning up the markets in this way. Something that is essential in the fight against OC.

The previously mentioned establishment of a bureau which combats black markets by disengaging licenses in order to wipe out OC has led to a law: The BIBOB-Act in 2003[5]. Furthermore, it was claimed that OC is not a strange phenomenon, but rather is also embedded in society as it needs licenses in order to flourish. Therefore, it could be the case that the authorities themselves further OC problems by issuing licenses. The law states that local authorities can seek advice at a national level in a special bureau in the Ministry of Justice to know who of the people asking for a license wants to take part in the bidding process in order to deny or even withdraw the license. If such strong measures are taken, there needs to be a particular degree of certainty that the public officials who apply these measures have proven their integrity. Accordingly, a special bureau only concerned with the integrity of officers was established.

3.2   The Developments in the Years 2007–2015

In 2006, the former mayor of Amsterdam, Job Cohen, caused an outcry by saying that a lot has been done, nevertheless, there are people in the city centre who have still a lot of criminal power, thus the national authorities have to be factored in. In 2007, the government passed a special policy program upon how to deal with the serious problems with regard to the levels of money laundering in real estate, but also the involvement of OC in prostitution and coffee shops in the City Centre District[6] which also stemmed the birth of the Emergo project. The project is a "[...] combined effort by the Municipality

---

[5] The law in other words allows local authorities to examine a person's or company's record before a license is issued. If there are reasonable arguments to come to the conclusion that a permit is being misused for criminal ends or may be misused in this regard, the license can either be withdrawn or be refused. Therefore, an (unintentional) involvement of the authorities in criminal activities is supposed to be prevented. For further information on the Public Administration (Probity Screening) Act (BIBOB) and its applications access: http://www.dutch-amsterdam.nl/259-bibob and Fijnaut, Paoli (2007): 677 et seqq.

[6] Also referred to as "1012" due to its postal code.

160

of Amsterdam, the City Centre district, the Amsterdam-Amstelland police force, the public prosecution service, the Tax and Customs Administration, and the Ministry of Justice" (Ministerie van Veiligheid en Justitie 2011: 284) and should integrate information as well as actions gathered during the analysis. Moreover, it was admitted that even after ten years of intensive research, the problem with reference to the identity of people and businesses taking action in OC was difficult to define. Therefore, even more importantly, as Amsterdam is one of the leading cities in the world, the 1012 district has to mirror a worthy appearance (Ministerie van Veiligheid en Justitie 2011: 283).

A whole strategy was developed by a task force – consisting of an "Enforcement Group", a "Serious Crime Group" and a group of researchers (Ministerie van Veiligheid en Justitie 2011: 284, 285) – in order to come to grips with this. In the framework of the Emergo project, for instance, very detailed analyses of specific streets in the red light district were made as well as detailed research on businesses in window prostitution, in the coffee shop system and in the low-rank hotels[7]. With the support of the local and tax authorities, an impressive integrated database was built which supported the identification of key players in the criminogenic markets. And in a number of cases, indeed, criminal law, fiscal and administrative action was taken against individual criminals, criminal networks or malicious businesses. As a complement the project focused on the reduction of opportunities in criminogenic markets e.g. in window prostitution or coffee shops and to strive for a more balanced economy and a more multifunctional society in the red light district. The execution of this sub-project reached from test borings to key figures to the rather radical revision of the zoning plan. Especially with regard to the cooperation between the diverse authorities involved in the Emergo project, it took more than a year before a legal framework was set up (Ministerie van Veiligheid en Justitie 2011: 286). In other words: it was in some respects not an easy project to do.

Nevertheless, the whole project demonstrates that the power of OC in metropolitan cities can be tackled fundamentally due to an identification of and action against criminal power structures and the reduction of the industries and markets they are embedded in.

---

[7] For further information consider the "Emergo rapport" by the Ministerie van Veiligheid en Justitie (2011).

Works Cited

Fijnaut, C. and Letizia Paoli. "Introduction to Part I: The History of the Concept." Organised Crime in Europe: Concepts, Patterns and Control Policies in the European Union and Beyond. Ed. Cyrille Fijnaut and Letizia Paoli. Dordrecht: Springer Science & Business Media, 2004. 21–47.

Kleemans, Edward. "Crossing Borders: Organised Crime in the Netherlands." Organised Crime in Europe: Concepts, Patterns and Control Policies in the European Union and Beyond. Ed. Cyrille Fijnaut and Letizia Paoli. Dordrecht: Springer Science & Business Media, 2004. 303–333.

Ministerie van Veiligheid en Justitie. Projectgroep emergo: EMERGO De gezamenlijke aanpak van de zware (georganiseerde) misdaad in het hart van Amsterdam. Amsterdam: Gemeente Amsterdam, 2011. Print.

The local Dimension of Cybercrime:
Report from a Trip to Râmnicu Vâlcea (Romania)

Federico Varese

University of Oxford

A constant refrain in both the academic literature and the popular press is that cybercrime is ubiquitous and liquid (e.g., Gabrys 2002. For relevant discussions, see Grabosky 2004; Wall 2007; Lusthaus 2013). Cybercriminals could attack you from anywhere; all they need is a terminal and a connection to the internet. I wish to dispute that view. Even this type of criminal activity relies on local ties in order to grow in size and reach.[1] These illegal enterprises are 'local in scope' (Reuter 1985: 21), although the victims are normally far from the perpetrators. It is not surprising that Russia is a highly conducing environment for internet-enabled thefts and illegal transactions. According to a recent study, the number of Russian underground forums grows every year. As of 2015, 78 websites are operating with 27% of them being "very active," and 41% being "active". Popular forums "can have 20,000 to several hundreds of unique members" (Goncharov 2015: 7). The same study indicates that prices for services offered on the forums have been dropping significantly (Goncharov 2015: 17). The virtual absence of state enforcement allows the market for stolen data to grow in size, and prices to become more competitive.

A country within the European Union that also appears to be a hub for cybercrime is Romania. Nicolae Popescu is on the FBI's Most Wanted list. Born in the small city of Alexandria, a two-hour bus ride south of Bucharest, Popescu is now in his early thirties. After organising a digital scam to sell hundreds of fictitious cars on eBay, and pocketing $3 million, he was arrested in 2010, but eventually was released on a technicality. He is now a fugitive from justice and the reward for any information leading to his capture is $1 million. Popescu is just one of the high-profile cybercriminals hailing from Romania. After controlling for the size of the population, Romania is the third country in the world for cyber-attacks (2013 data by Bloomberg. See Milian 2013).[2] Why?

---

[1] On the local nature of other forms of organised crime, see Reuter (1985) and Varese (2011). Normally, the opposite view is argued by Shelley (2006) and Williams (2001).

[2] According to the U.S. Embassy in Bucharest, Romanian cybercriminals steal $1 billion every year by targeting US computers (Odobescu 2014).

The aim of this short essay is to offer a preliminary answer to this question and to underline the *local* nature of large-scale cybercrime.

Part of the answer is the legacy of communism. The regime of Communist dictator Nicolae Ceausescu had invested significant resources into computer science studies. As the country was denied access to Western technology, in addition to technology from the USSR, Romanians developed their own IT capabilities, including reverse–engineering a microprocessor. This legacy has largely been positive: many of those young people are now working in London, Silicon Valley and Seattle, while several American companies develop software and Apps in Bucharest. BitDefender, based in Bucharest, is the Romanian company that produces one of the world's most widely used antivirus systems. In the early 1990s, there were hundreds of home-made micro-networks in the country. This explains how Romania came to be the nation with the fifth fastest Internet connection in the world. Those who live in the city of Timisoara, Western Romania, have the fastest network on the planet (Polat 2012). This level of connectivity is crucial for the so-called "Denial-of-Service-Attacks", but also for many virtuous purposes. While Romania has a high level of IT expertise, it remains one of Europe's poorest countries. The 2014 average salary is 398 Euros a month (the EU average is 1,489), while agriculture is not fully mechanised: there are 201 tractors per 100 sq kilometres of arable land (the EU average is 815.1).[3]

Not all parts of Romania are equally affected by cybercrime. Table 1 presents data from Romania Court of Appeal related to internet fraud (*fraudă informatică*) for the period 2008–2010 (when data are available).[4]

---

[3] Data from http://www.reinisfischer.com/average-salary-european-union-2015 and http://wdi.worldbank.org/table/3.2.

[4] Jurindex is a free service which aims to provide free access to judgments of courts. All courts of appeal decisions published in the period 2008 – February 28, 2010 in JURINDEX. There are a total of 233,921 documents.

Table 1. Number of decisions of the Court of Appeal for cases involving "fraudă informatică", 2008–2010, Romania.

	Number of cases	% of total
CA PITEŞTI	75	26.98
CA BUCUREŞTI	38	13.67
CA BACĂU	25	8.99
CA CLUJ	22	7.91
CA BRAŞOV	21	7.55
CA CRAIOVA	19	6.83
CA ALBA IULIA	18	6.47
CA GALAŢI	16	5.76
CA TIMIŞOARA	11	3,96
CA IAŞI	10	3.6
CA CONSTANŢA	9	3.24
CA PLOIEŞTI	9	3.24
CA SUCEAVA	4	1.44
CA ORADEA	1	0.36
CA TG MUREŞ	0	0
CA MILITARĂ	0	0
TR VRANCEA	0	0
Total	278	100

Source: Jurindex, http://jurisprudenta.org

Table 1 indicates that the region of Piteşti accounts for 27% of all cases. The Court of Appeal located in the region of Piteşti has jurisdiction over the town of Râmnicu Vâlcea.[5]

On paper, the economic situation in Râmnicu Vâlcea is dire. OltChim, the company owning the large chemical plant built by the communist regime in 1966, went bankrupt in 2012, yet the regional GDP continues to grow (INS-RV 2014). When I visited the town in March 2015, I noticed trendy cafes, bistros and restaurants in this town of 92,000 inhabitants. I stopped at the Academy of Taste, a gastro pub specialising in Italian food. My hotel, built

---

[5] Information based on police investigations, provided by Maxim Dobrinoiu, suggest that over 70% of cybercrime occurs in the Southern and Eastern Romania.

three years ago at a cost of 3.5 million euros, boasts a Spanish chef and the room spacious and comfortable (it is located right in front of the dilapidated police station). Signs of private wealth abound in town: two shopping centres located on the main square has five floors of shops selling designer clothes, appliances, computers, sporting goods, jewellery, as well as hosting a cinema, restaurants, bars, beauty centres, and bakeries. A dealership of Mercedes-Benz, is a nearby village. What is the source of such wealth? Several newspaper reports have suggested that Râmnicu Vâlcea is a hub of internet frauds (Wylie 2007; Bhattacharjee 2011; Bran 2011; Hall 2014; Dunne 2015).[6]

From the middle of the 1990s, Râmnicu Vâlcea has become known for internet scams. Initially victims were sold non-existent items on EBay. Soon, Western consumers begun to be suspicious of sellers from Eastern Europe. This is when online scams became more sophisticated. Vendors now appear to reside in the United States or England, and payments are directed to reputable banks. Every detail of the scam is credible. The head of the Computer Unit of the Police showed me a highly polished website offering to rent holiday apartments and villas, equipped with a section for reviews. When the customer contacts the landlord, s/he is willing to send copies of documents confirming the ownership of the property and is even willing to describe on the phone the amenities of the resort. To enhance its credibility, the agency allows the customer to pay through an escrow service, also bogus. Fax numbers used in official correspondence do not correspond to any land line telephone: software converts incoming faxes into emails (I1).

Once the money has been paid into accounts based in Western banks, and somebody – known as 'arrow' – has taken the cash out, the fraudster needs to send the proceeds of crime to Romania. Money transfer agencies are the most popular way to repatriate the cash to Râmnicu Vâlcea.[7] There are several precautions to follow: the amount should not exceed 5,000 euros and the receiver should not use the same branch to collect the money too often (I2). During my visit to the town, I stopped for about an hour to observe the line at the counter of a Western Union shop on the ground floor of one of the town shopping centres: young people, women, children and old people withdraw money, talked, greeted each other and vanished into the meanders of this unlikely cathedral of consumerism. A few meters away there was the subsidiary of MoneyGram.

---

[6] Curiously, a small cottage industry for foreign journalists and filmmakers has emerged in Râmnicu Vâlcea. It did not take long for me to be approached by a fixer willing to offer introductions to the dark world of hackers in town, for a hefty fee. Such 'service' appeared to be a scam itself.

[7] Information based on police investigations, provided by Maxim Dobrinoiu.

As shown in Table 2, there are 64 branches of Western Union in Râmnicu Vâlcea, one for every 1,446 inhabitants. For comparative purposes, I calculated the number of branches per inhabitants for Bucharest (one every 8,118 people), Novara, Italy, a city with roughly the same population (one for every 4,375 inhabitants) and Alessandria, Italy (one for every 2,415 inhabitants). The data suggest that the number of Western Union branches in Râmnicu Vâlcea greatly exceeds that of other cities in Romania and Italy. Similarly, the number of MoneyGram branches in Râmnicu Vâlcea is 13, one for every 7,121 people. In Bucharest, the same company has 70 branches, one for every 26,906.

Table 2. Number of Western Union Agencies in selected cities.

Cities	Number of Western Union (WU) shops	Population	WU/ population
Râmnicu Vâlcea	64	92,573	1,446
Bucharest	232	1,883,425	8,118
Focşani	47	73,868	1,571
Braşov	127	369,896	2,912
Târgu-Mureş	62	134,290	2,165
Novara (Italy)	24	105,000	4,375
Alessandria (Italy)	39	94,191	2,415

Source: http://www.westernunion.co.uk/gb/Home.page

According to local prosecutors, there are at least a thousand people working full time on computer frauds in town, mostly based in just one neighbourhood, Ostroveni. A *Le Monde* correspondent wrote in 2011: "In Ostroveni, everyone knows what is happening, but omertà – the code of silence – is the norm" (Bran 2011). Allegedly, High School no. 10 in the Ostroveni district of town is the place where hackers and scammers first cut their teeth.

The groups are organised on the basis of a strict division of labour: young computer enthusiasts are recruited by criminal minds capable of using violence.[8] Earnings can be significant: a gang arrested a year ago had made in a short time a million and 400 thousand euros (Hall 2014). These gangs benefit from of a *local* network of contacts and protections. The 'arrows', who withdraw the cash in London, and transfer it back to Romania by car or plane or

---

8   Information based on police investigations, provided by Maxim Dobrinoiu.

send it through Western Union, have a personal knowledge of local gang leaders.[9] Meeting in person is an effective strategy to build trust in illegal markets.

A key ingredient for the persistence of functioning illegal enterprises is local corruption. The Deputy Head of Râmnicu Vâlcea police, Gabriel Popa, was arrested in December 2014 for revealing confidential information to a gang of criminals. On 20 March 2015, another police officer, Alexander Popa, accused of passing confidential information to a cyber gang led by Nicolae Vasile, was also arrested. This clan has recently netted almost 200,000 Euros from frauds involving about 600 British victims. The penalty for the two officials was 30 days under house arrest (Rîpan 2015). Occasionally the police are successful at arresting lawbreakers, making the case of Romania less extreme than that of Russia.

Politicians also are involved. The socialist senator elected in Râmnicu Vâlcea, Laurenţiu Coca, was heard speaking on the phone with Mihai Obreja, the boss of a local gang that, in addition to cybercrime, is involved in loan sharking and extortion. The conversation between the two men was far from friendly: "Return the money you've come to take to my house, or you're fucked," said Obreja to the Senator (Miercuri 2015). In another phone intercept, a member of the same gang is heard threatening to cut off the hands of a victim who has not yet repaid his debt (Miercuri 2015). As evidence that corruption is widespread in the valley, Râmnicu Vâlcea's mayor (elected in 2012) was convicted to 4 years for bribe taking in 2014 (Jurnalul Naţional 2014). Those who expose the links between organised crime and local political elites are threatened and assaulted. This is what happened to Romeo Popescu, the owner and editor of the local newspaper *Vocea Valcii* (Hall 2014). Today the newspaper has changed location for security reasons.

This essay is a preliminary exploration of the factors that facilitate the growth of cybercrime. I have argued that large-scale cybercrime thrives thanks to social networks, in places where the local institutions are weak and corruption is widespread. Ultimately, the lack of effective enforcement is the most important factor affecting the growth of cyber-related illegal enterprises. The policy implications of this argument are twofold: while the victims are thousands of kilometres away and surely need to be vigilant, the eradication of the cybercrime industry depends also on effective local governance.

---

[9] Information based on police investigations, provided by Maxim Dobrinoiu.

1   Acknowledgments

Bibliography

Interviews

I1. Interview with officer from Cybersecurity Unit, Bucharest, 21.III.2015.
I2. Interview with person active in the Romanian cyber world, Bucharest, 22.III.2015.

Newspaper Articles

Bhattacharjee, Yudhijit 2011. How a Remote Town in Romania Has Become Cybercrime Central. *Wired Magazine*, 31 January.

Bran, Mirel 2011. Les pirates roumains d'"Hackerville" tiennent tête aux polices du monde entire. *Le Monde*, 28 December.

Hall, Allan 2014. The scourge of Scamville: Romanian town is the cyber-crime capital of the world – where hundreds of fraudsters rake in millions from gullible online shoppers. *Daily Mail*, 21 November.

Jurnalul Naţional 2014. Primarul din Râmnicu Vâlcea, Emilian Frâncu, condamnat definitiv la 4 ani de închisoare cu executare. *Jurnalul Naţional*, 26 March.

Miercuri 2015. Senatorul PSD Laurenţiu Coca implicat în afaceri cu Labuş. *Miercuri*, 14 January.

Milian, Mar. 2013. Top Ten Hacking Countries. *Bloomberg Business*, 23 April. Available at: http://www.bloomberg.com/slideshow/2013-04-23/top-ten-hacking-countries#slide5.

Odobescu, Vlad. 2014. U.S. data thefts turn spotlight on Romania. *USA TODAY*, 13 January.

Polat, Anil 2012. Why Is the Internet in Romania So Damn Fast? 15 March, available at: http://foxnomad.com/2012/03/15/why-is-the-internet-in-romania-so-damn-fast/.

Rîpan, Irina 2015. Caz inedit în poliţia vâlceană: Alexandru George Popa, primul poliţist arestat la domiciliu pentru 30 de zile. *Adevarul.ro*, 21 March.

Wylie, Ian 2007. *Romania home base for EBay scammers*. Los Angeles Times, 26 December.

Reports

Goncharov, Max 2015. Russian underground. TrendLabs research paper. Available at: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/wp-russian-underground-2.0.pdf

INS-RV (INSTITUTUL NAŢIONAL DE STATISTICĂ, DIRECŢIA JUDE-ŢEANĂ DE STATISTICĂ VÂLCEA) 2014. *Anuarul Statistical Judeţului Vâlcea 2014*.

Video

Dunne, Sean 2015. *In Search Of The Most Dangerous Town On The Internet*. Norton Productions, 20 m. Available at: https://www.youtube.com/watch?v=un_XI4MM6QI

Academic studies

Gabrys, Ed 2002. The International Dimensions of Cyber-Crime, Part 1. Information Systems Security, 11:4, pp. 21–32.

Grabosky, Peter 2004. The Global Dimension of Cybercrime. Global Crime 6(1), pp. 146–157.

Lusthaus, Jonathan 2013. How organised is organised cybercrime? Global Crime 14(1), pp. 52–60.

Reuter, Peter 1985. *The organization of illegal markets: An economic analysis.* New York: U.S. National Institute of Justice.

Shelley, Louise 2006. The globalization of crime and terrorism. eJournal USA 11 (1), pp. 42–45. Available at http://www.america.gov/media/pdf/ejs/ijge0206.pdf#popup.

Varese, Federico 2011. Mafias on the Move. Princeton UP.

Wall, David 2007. Cybercrime: The Transformation of Crime in the Information Age. Polity Press.

Williams, Phil 2001. Transnational criminal networks. In Networks and netwars: The future of terror, crime, and militancy, ed. John Arquilla and David F. Ronfeldt, pp. 61–97. Washington, DC: Rand Corporation.

Corruption and Organised Crime Threats in Southern Eastern Europe

Ugljesa Zvekic

Global Initiative against Transnational Organized Crime

1   Organised Crime and Corruption in the Global Developmental Perspective

In this article the emphasis was on a nearly inherent link between organised crime and corruption on a local as well as transnational level. Wherever there is ground prone to corruption, there is also a favourable ground for organised crime; and vice versa. Much of the prone ground for organised corruption is established through firstly a low corruption level which then accelerates to a more sophisticated level of corruption, in particular when linked to organised crime. Furthermore, it was professed that today more intricate activities in organised crime can be linked to more intricate activities in corruption, making them mutually instrumental.

Historically speaking, two contradictory trends were identified: Firstly a decline in violent crimes over the past century and decades, and secondly an increase in global organised crime and corruption, which in turn promoted more international legal responses and cooperation. (Pinker, Mack 2014/2015) The phenomenon of organised crime is not new to the global crime trends but the scale and scope have shifted vigorously. Change is also presents in new forms and methods of legitimizing illicitly gained profit. The impact comes to light in the form of shifts in major illicit markets, an expansion of new criminal markets as well as a blurring of traditional producer, consumer and transit state typologies. Therefore, organised crime and corruption both have broader implications than defined within the traditional security and justice framework; hence they are now recognised as cross-cutting threats to a sustainable development which is also pictured by the 16th goal of the Sustainable Development Goals[1].

---

[1] https://sustainabledevelopment.un.org/focussdgs.html: "16. Rio+20 reaffirmed that, in accordance with the Charter, this shall not be construed as authorizing or encouraging any action against the territorial integrity or political independence of any State. It resolved to take further effective measures and actions, in conformity with international law, to remove obstacles and constraints, strengthen support and meet the special needs of people living in areas affected by complex humanitarian emergencies and in areas affected by terrorism."

With regard to corruption, the least corrupt countries as per the Transparency International (TI) Corruption Perception Index (CPI) e.g. the Scandinavian countries and New Zealand are also the most stable politically and economically with an efficient public administration; on the other hand, the countries most vulnerable to corruption, such as South Sudan and Somalia, are quite unstable in terms of economy and politics. Thus, it is not the corruption per se – rather, the context in which the corruption vulnerability or resistance has to be looked at. Despite much criticism regarding the TI CPI[2] due to its methodology and an "elite bias"[3], the CPI has achieved an important political aim: to acknowledge corruption publicly as a major problem on international level to an extent that governments from every country are eager to see and improve their ranking in the CPI. The CPI became a very powerful, methodological, even more importantly political tool for acknowledging corruption on different levels.

According to TI, the most vulnerable institutions for corruption are political parties, the police and public administration, which is quite worrisome, as those who are supposed to exercise control and to monitor the system are globally perceived to be the most vulnerable institutions to corruption. Special worries regard the perceived corruption of parliament and judiciary. On the other hand, the most vulnerable economic sectors are construction, extraction and transport which in many countries still are state-owned or public agencies. Organised crime is very much present in those sectors for which public bids are made and it is known that the link between organised crime and corruption is often established there.

1.1   Corruption and Organised Crime in the Regional Perspective: The Western Balkans

The discussion of corruption and organised crime will focus on the Western Balkans, namely Albania, Bosnia and Herzegovina, Montenegro, Serbia and

---

2   The CPI lists countries and territories according to their perceived corruption in the public sector. It is a combination of polls, relying on corruption-related data collected by trustworthy institutions. The index reflects the views of observers from around the world, including experts living and working in the countries and territories evaluated (http://www.transparency.org/cpi2014/in_detail#myAnchor1).

3   Referring to the critique of lacking validity due to the reliance on perceptions, Transparency International states: "There is no meaningful way to assess absolute levels of corruption in countries or territories on the basis of hard empirical data. Possible attempts to do so, such as by comparing bribes reported, the number of prosecutions brought or studying court cases directly linked to corruption, cannot be taken as definitive indicators of corruption levels. Instead, they show how effective prosecutors, the courts or the media are in investigating and exposing corruption."

Kosovo[4]. According to the CPI, in 2014 the perceived level of corruption in the Western Balkan region illustrates that the majority of countries from the Balkan region are located on an average level with ranks from 64 to 80 out of 175 points. Albania as well as Kosovo stand out, both with a rank of 110. It is important to note that South Eastern Europe is equally divided among five EU members (Greece, Slovenia, Bulgaria, Romania and Croatia) and the non-EU members (The Western Balkans); on average, the EU members have much better TI ranking than the non-EU members which points out that reducing public administration corruption, which is usually reflected through the TI CPI, is one of the requirements to join the EU and it can be met.

In accordance with the findings from TI but also the UNODC surveys (2010) on both population and businesses in the Western Balkan region, bribery has one of the highest prevalence rates (ca. 13%).

Figure 1. Annual prevalence rates for different types of crime.
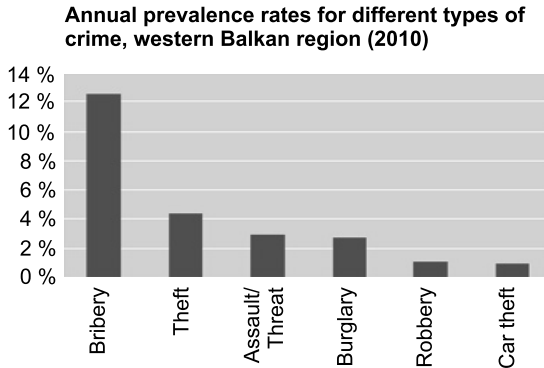
Annual prevalence rates for different types of crime, western Balkan region (2010)

Source: UNODC (2011), "Corruption in the Western Balkans:
Bribery as experienced by the Population"

The second crime field which is mostly prevalent in the western Balkan region is "Theft" with a prevalence rate of slightly over four per cent. "Theft" is closely followed by "Assault/Threat" and "Burglary", both with prevalence rates of about 3 per cent. The tail lights consist of "Robbery" and "Car theft" both accounting for 1 per cent of crimes. What should be noted is the enormous difference of eight percent points regarding the occurrence of conventional crimes like theft or even assault, on the one hand, and bribery, on the other. Corruption is therefore a serious issue in the context of security.

---

[4] Kosovo as per the UN Security Council resolution 1244.

Further, it was outlined that the most important issues in the Western Balkan region are perceived to be unemployment (33%), poverty (20%) and then corruption (19%). Another outstanding issue concerns the performance of the government (15%), which may also be connected to the aforementioned issues. Infrastructure, education, the environmental deterioration and ethnic equality concern few Balkan adults. It appears that corruption is ranked very high on the agenda of public opinion.

Figure 2. Prevalence distribution of bribes paid, by purpose of payment (2012).
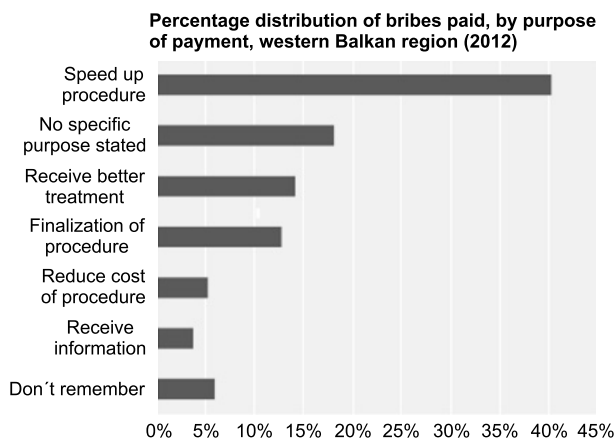
Percentage distribution of bribes paid, by purpose of payment, western Balkan region (2012)

Source: UNODC (2013), "Business Corruption and Crime in the Western Balkans: The Impact of Crime and other Bribery on Private Enterprise", p. 28

For ordinary citizens, bribery is used as an effective instrument: to speed up procedures, to receive better treatment, the finalization and to reduce cost of a procedure and to receive information. Further, a connection with illicit elements and those who pay bribes is always visible, for corruption is mostly a partnership composed of a corruptor and a corrupted. As a result, the centre of the problem was located in public administration as to make it function efficiently for the clients, it needs to be bribed.

Within the public administration sector there are certain occupational categories and public institutions that are more vulnerable to corruption.

Figure 3. Prevalence of bribery by public officials receiving the bribe.

**Prevalence of bribery by public officials receiv-
ing the bribe, western Balkan region (2010)**

Source: UNODC (2011), "Corruption in the Western Balkans:
Bribery as experienced by the Population", p. 25

Public officials receiving bribes are mostly police officers but also doctors
and customs officers as well as judges or prosecutors.

177

Figure 4. Percentages distribution of bribe-paying businesses that pay bribes to selected types of public official

Percentage distribution of bribe-paying businesses that pay bribes to selected types of public official, western Balkan region (2012)

Category	
Municipal or provincial officers	
Tax/revenues officers	
Customs officers	
Public utilities officers	
Police officers	
Inspection officials	
Land registry officers	
Health authorities	
Municipal or privincial elected representatives	
Other public official	
Social protection agency/ministry officers	
Judges/Prosecutors	
Members of Parliament/Government	

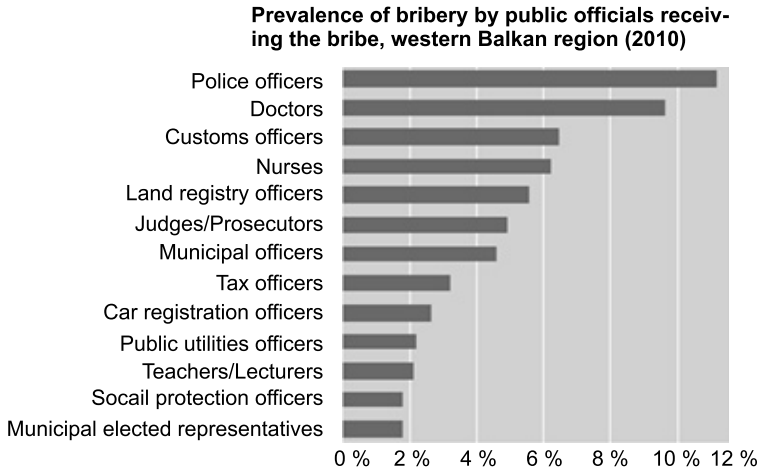0 %   5 %   10 %   15 %   20 %   25 %   30 %
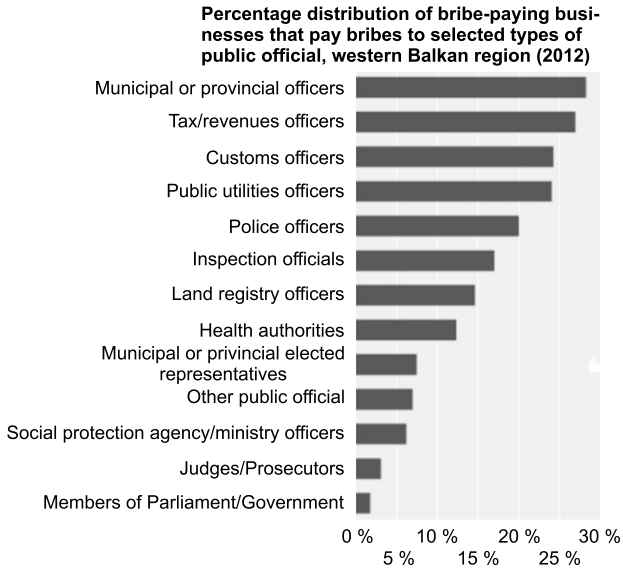
Source: UNODC (2013), "Business Corruption and Crime in the Western Balkans: The Impact of Crime and other Bribery on Private Enterprise", p. 30

Not only citizens, but also businesses pay a vast amout of bribes to public officials as well.. Correspondingly, nearly 30 per cent of bribes paid by businesses are directed towards municipal or provincial officers, closely followed by tax/revenues officers (27%). Members of the parliament or government as well as judges or prosecutors are among the least bribed public officials at less than 5 per cent. As a result, it was stated that the largest share of bribes is paid to local public officials, further reinforcing the impact corruption exercises on the public admnistration sector including tax revenues.

As pointed out above, much of the corruption perceived is centred on public administration in the Western Balkans which clearly identifies it as a target for much of the anti-corruption work – in particular in view of joining to the EU.

1.2 Police Sectors vulnerable to Corruption and Forms of Police Corruption in Serbia

It is noteworthy that not all sectors of public administration are affected by corruption to the same extent; the more public officials certainly engage with the public, the more serious the case at stake, the more likely that some form of bribery may take place. It also depends on the position and function the public official enjoys. Specifically for Serbia, some police sectors vulnerable to corruption were examined: among the most common sectors are traffic police (75%) and economic crime (71%) as well as border police (68%), criminalistics (59%) and the ministry of interior (47%) but also special police units, mostly concerned with anti-drug cases (32%); whereas the latter is traditionally most exposed to corruption.[5]

The forms of police corruption are singled out as follows: bribery by criminals for favours regarding their sentence or fine (47%), bribery by citizens e.g. if they need some administrative document (23%), selling of "secret investigative" information usually to the defence in preparation of the trial (6%). These are very serious indicators of the weaknesses of the police sector in Serbia. Correspondingly, the utmost priority areas for police reforms considered important are: increasing the accountability and fighting corruption in police.

2 Concluding Observations: Political Economy of Organised Corruption

Corruption is becoming less and less an individual act as there is a need for organisation, division of labour and for people who act, launder and in the end, legalize the profits. The distinction between active and passive corruption is fading to an increasing degree. The process occurring in the Balkan region was fuelled by the fall of the Berlin Wall which enormously affected the rest of the world. Respectively, the part of Eastern Europe experienced a "wild-west" privatization which refers to the ex-communist party nomenclature and organised crime buying formerly state-owned real estate like factories, enterprises and land. This process led to the legalization of the representatives of the old regime and organised crime in a new environment as businessmen and still affects the ability to prevent and control organised crime and corruption. On the other hand, organised crime in the Balkan region was traditionally involved in drug trafficking and smuggling of cigar-

---

5 Sasa Djordjevic, Riba se cisti od glave, Weekly "Vreme", 23 July 2015 (based on a research project "Integrity and the Trust in the Police in the Western Balkans", sponsored by the EU).

ettes and later on also focused on human trafficking and arms trafficking (in particular during the Yugoslav wars). Attention was also called to the process of legalizing profit through money laundering. In the real estate business, banking, gambling industry and the financial markets. Corruption plays an important instrumental role in the process of the legalization of illicit gains. The main problem we will face in the future is the fact that when organised crime enters the market, it starts buying shares in companies. Moreover, it was warned that this phenomenon is particularly difficult to fight on a local and on an international level and will require more partnerships with corporate sectors, thus demanding the companies to take responsibility for the illicit flow of money within their enterprise. Furthermore, this would pose the problem of interference of the government in the market economy which is a completely different economic model that might be prompted by the penetration of the new modalities of operation of organised crime and corruption.

In summary, organised crime and corruption go hand in hand. This is particularly evident in the Western Balkans with certain levels of political and economic instability. The Yugoslav war and the privatization of the economic sector provided ample opportunities for organised crime to launder, to corrupt and to legalize its presence. Today it is no longer the question of police and judicial capacity anymore to tackle organised crime and corruption. It is the matter of political commitment and good public and corporate management – good governance.

Eurasian Organised Crime Structures in Germany – Countermeasures and Efforts of German Law Enforcement Agencies

André Schünemann

Bundeskriminalamt Germany

1   Introduction

Organised crime and its connected networks are involved in many different criminal activities around the globe. Eurasian organised crime[1] is no exception – it consists of a complex criminal organisation and phenomenon that became particularly sophisticated after the collapse of the Soviet Union (Webster, 1997). Radical changes in the political system and landscape during the early 1990s left an economic, moral, and social vacuum which resulted in manifold opportunities for organised criminal activities to flourish throughout the different republics of the former Soviet Union (Frisby, 1998). Hence, in many former Soviet republics, independence and self-determination not only led to a fundamental transition of social, political, and economic power, but also to the emergence of the phenomenon of Eurasian organised crime.

Vory-v-zakone, which is the Russian name for the thieves-in-law, are high-ranking professional criminals within the Eurasian organised crime structures (Slade, 2012a, p. 624). The fraternity of the thieves-in-law and its specific code of conduct emerged from the Soviet prison labour camps (Gulags), mainly during the Stalin era. Later on, during the era of the 1980s when the Soviet economy was stagnating, the thieves-in-law and their criminal organisations began to fill gaps and shortages by establishing a "shadow economy" and provided goods and services to society. While these activities also involved state actors on different levels within the Soviet system, these linkages enabled the thieves-in-law to sustain and expand their influence during and after the collapse of the Soviet Union (Kegö & Molcean, 2011, p. 14 et seqq).

---

[1]   Instead of using *Russian Organised Crime,* the broader term *Eurasian Organised Crime* is used in order to incorporate the collective of various organised crime groups, which originate from the entire former Soviet Union.

2 Elements and the hierarchy of Eurasian organised crime

The thieves-in-law and the structures subordinate to them represent one of the most important elements of Eurasian organised crime. The model used is a simplified representation of the structure associated with the thieves-in-law – other authors drafted various models (e.g. Fedpol, 2010, p. 10; Lungren, 1996, Chapter Organization and Structure; Slade, 2013, p. 96).

Figure 1. Hierarchy and Elements of Eurasian Organised Crime.
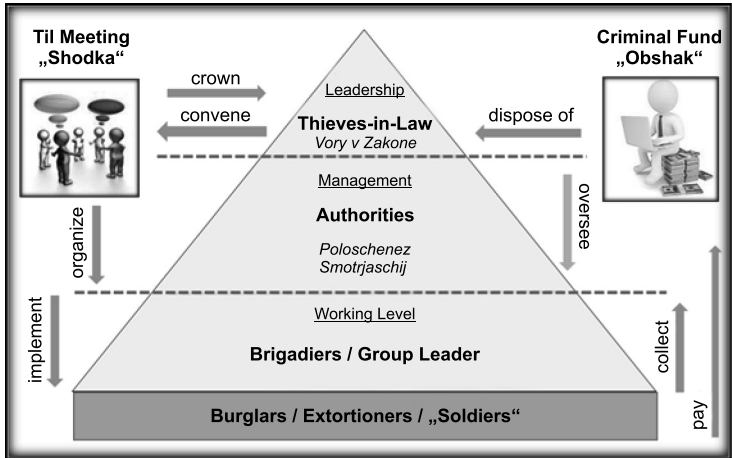
Source: Bundeskriminalamt Germany (2015)

The established thieves-in-law, who are career criminals, occupy the top of the pyramid – they are responsible for various fields of activity that can be tailored to certain areas of crime or regions. Besides this, there is a clear hierarchy within this group. Information indicates that the highest-level includes representatives of the thieves-in-law but also leaders of the large syndicates which form a committee. This committee is sometimes labelled as "The Brothers' Circle" – a multi-ethnic group of senior, and powerful, criminal members of former USSR, including key figures of the thieves-in-law (Cohen, 2011; Kattge, 2014, p. 196). In this leadership committee thieves-in-law and others meet on strategic issues, decide on territories and fields of responsibility, and solve problems.

Besides, the thieves-in-law are spread around the globe and are able to conduct their illicit business from any place in the world. However, for their operational activity in local areas an authority (known as *smotryashii*) serves as

a confidant and trustee (Slade, 2013). These *smotryashii* form what might be called the management level. In the level below, called the working level, the brigadiers or group leaders are active in specific regions or crime areas. They are responsible for operations and are in charge of workers or "soldiers", whom they assign to the specific fields of criminal activity.

The *obshak* – the communal and social fund – serves as a shared and unifying element. Money is collected in this fund by the next higher level of the hierarchy, money that, through clearly specified and defined channels, ultimately ends up at the disposal of the thieves-in-law. This fund provides support for the members, but also for the thieves-in-law who use it to finance their lifestyle. The payments to the communal fund are usually voluntary. Those further down in the hierarchy submit to this system because they know that such payments also have a protective function: for their own illegal activities and as a form of "social security" in case they are arrested (Kegö & Molcean, 2011, p. 13; Slade, 2012a, p. 629). Obshak payments are accepted within these criminal groups which are led by thieves-in-law.

Internal agreements within thieves-in-law are reached at special meetings (known as *shodka*), which are a type of "leadership" or "management" conferences. These meetings are called mainly to promote individuals to the rank of thief-in-law, known as a "crowning", and/or sometimes to mediate in the case of conflicts between thieves-in-law and/or their subordinates. It is an organ of internal control and representation (Rahr & Pachomow, 1998; Slade, 2012a; Slade, 2013; Varese, 1998). In particular, the results of these meetings – which at times are organised by subordinates or confidants of the thieves-in-law – are ultimately binding and subsequently implemented at the lower levels.

3   Situation in Germany

Germany and its neighbouring countries, due to their central location in Europe, and not least due to the freedom to travel, are an interesting area for criminal activities. The Russian-speaking segment of the population in Germany is relatively large at 4.5 million persons due to the large numbers of Russian-speaking migrants settling over the years. In addition, officially about 19,000 Georgian nationals live in Germany. According to information held by the police, the thieves-in-law are also active in Germany, as well as other criminal groups and syndicates associated with Eurasian organised crime. Regarding the thieves-in-law and their ideology, it should be noted that on average between 4,500 and 5,500 prison inmates in German penal institutions also subject themselves to the specific code of the thieves-in-law. The code of conduct, and the domination-subordination relationship asso-

ciated with it, is implemented and practiced within this group of persons – who, even though they do not enjoy "real" status, nevertheless adopt the code. This is particularly problematic because these persons naturally do not remain in custody indefinitely. While still in prison, they establish the inherent structures, and thus, also establish these structures within German society when they are released. Ultimately, the structures and the associated conduct persist outside German prisons.

Police information indicates that, in their entirety, Eurasian organised crime structures have spread and become more firmly established in recent years (especially after the fall of the Berlin Wall). Concerning the various Eurasian/ Russian-speaking groups, structured procedures, cooperation and coexistence between them is observable. Furthermore, this also applies to other national and/or ethnic groups in the field of organised crime – they support each other when it is sensible and opportune.

Further, information on hand indicates that Germany is divided into individual areas of influence among the thieves-in-law which is based on type of criminal activity and/or regional criteria. Despite this, the public largely lacks fundamental awareness of Eurasian organised crime structures. On the one hand, these due to the groups try to avoid public attention when pursuing their criminal activities in secret. On the other hand, the individual leadership and decision-making levels are insulated from each other, while the organisation as a whole is insulated from the world outside. For this reason, even law enforcement entities are often not able to recognise Eurasian organised crime structures until, for example, conflicts become public. Besides, in the case of Eurasian organised crime, nearly all forms of criminal activity are represented, and more recently, highly professional Caucasian groups are particularly active in the field of property crime.

4 Activities and criminal offences of Georgian organised crime groups in Germany

In order to examine details of criminal conduct of Georgian criminal groups, some facts on the crimes themselves are relevant.

4.1 Petty Offences – Shoplifting by organised crime groups

Shoplifting is an example of high-volume crime and, the question is, to what extent shoplifting represents a form of organised crime. In this regard, it should be noted that both the police and the retail industry assume the number of undetected and/or unrecorded cases to be relatively large. In total in 2014,

there were 365,373 cases of shoplifting in Germany committed by 260,131 suspects. The clearance rate is about 92% (BMI, 2015, p. 4, 80). This is because the offence is usually reported to the police when a shoplifter is caught. However, it can be assumed that unreported cases exist: within the chain of delivery, storage and, finally, display of merchandise in a store, it often cannot be clearly established when and where merchandise is stolen or goes missing.

When considering shoplifting, it is notable that from 2013 to 2014, a significant increase, exceeding 48%, for Georgian shoplifting suspects (to about 3,700) was recorded. However, Georgian suspects represent only 1.4% of all suspects. Nevertheless, if the figures for reported crime committed by Georgian shoplifters are examined, the losses are relatively large: it is assumed that a Georgian shoplifter is active about 200 days a year and causes losses of about 500 Euros per day (Mayr, 2012). Using the figure of about 3,700 suspects, based on the reported crime numbers, 370 million euros can be estimated as the amount of loss.

4.2 Domestic Burglary by organised crime groups

Domestic burglary is another field of criminal activity of Georgian criminals. In this area of crimes, an unfortunate correlation between a large number of offences (152,123) and a relatively low clearance rate of 15.9% in 2014 (BMI, 2015, p. 53) can be observed. With regard to Georgian suspects, there was a significant increase of 122% from 2013 to 2014. But, within the total number of domestic burglary suspects (17,051), the proportion of Georgian offenders is only 2.15%.

However, reports from a number of federal states coincide in regard to shoplifting and domestic burglary: Georgian nationals registered in Germany as asylum seekers are actively engaged in these fields of criminal activity (Focus, 2015; Wiermer, 2015). Since 2011, the number of asylum seekers from Georgia has continuously increased to more than six-fold at above 3100 Georgian asylum seekers in 2014. The current figures for the period until July 2015 indicate that the present trend is continuing, at least at the same high level. For Georgians, this is of particular interest because the quota of granting asylum (the protection rate = percentage of those granted asylum) decreased from 2.1% in 2011 to almost 0% in 2014/2015 in Germany. In brief, there is generally no legal ground for Georgian nationals to seek asylum in Germany. However, the current trend is in the opposite direction.

Currently, extensive Europe-wide measures are pursued against organised groups of Georgian shoplifters, and the Spanish authorities arrested burglars controlled by Georgian thieves-in-law in March 2010 (Oxford Analytica,

2010). Furthermore, various European police authorities have recently determined that Georgian gangs of shoplifters and burglars in Europe still operate under the "roof" of protection of Georgian thieves-in-law. Thus, a problem arises for German and European authorities with regard to such petty crimes – namely that individual offences in areas of high-volume crime are not recognised as part of organised crime structures controlled from the higher levels of a hierarchy. Instead it often has been, and still is, assumed that these are individual offences unrelated to other crimes.

4.3   Countermeasures and Efforts of German authorities

The increasing numbers of property crime, particularly shoplifting and domestic burglaries resulted in major security priorities of police, namely combatting organised property crimes, as well as a focus of attention of levels of government.

By jointly concentrating efforts on Georgian offenders, German police agencies of various federal states, the Federal Criminal Police Office, the Federal Police (regarding border police related issues), security agencies at the state and also the federal government level, and the Federal Office for Migration and Refugees have created a multi-agency project. Objectives of this multi-agency working group are to identify and break up groups of Georgian criminals, as well as their logistic structures, and to establish information that serves as evidence of a connection between Georgian gangs of petty criminals in Germany and the higher-level structures of Georgian thieves-in-law which are part of Eurasian organised crime. A further objective is to establish a nationwide, multi-agency crime-fighting network to thereby optimise international cooperation and facilitate combating such groups of criminals as effectively as possible.

Thus, a number of measures need to be implemented and necessitate the coordination of national and international activities. Among others, a centralised analysis of data about Georgian criminals in order to identifying relevant key players – namely persons who, for example, serve as logistics specialists with regard to dwellings, motor vehicles, or other forms of support, and who therefore stay in Germany for longer periods of time. In addition, the analysis aims at identifying offence-related and structural connections involving groups of persons in Germany, as well as in other parts of Europe. All these measures are naturally also aimed at either initiating an investigation against criminal groups, which have been identified, and at providing support for investigations conducted by other authorities. In detail, the process functions of this multi-agency working group is that information available on Georgian nationals – from national as well as international partners – is gathered, com-

piled/compared and processed at a single point of contact. As a result, multiple matches or cross-matches (of various data items) are utilised to analyse committed crimes and its patterns in more detail. Moreover, subsequent analytical cross-match reports are made available for relevant project partners. In this regard, the cooperation with foreign authorities and international agencies is crucial for the project and it utilises, for example, Europol for a structured multilateral cooperation (Kattge, 2014, p. 198). Finally, all the information gathered enables the project team to identify national and transnational links and associates of a highly mobile criminal group of Georgian offenders, and its management and leadership levels, such as responsible thieves-in-law. As a result, the project hypothesis that the thieves-in-law control Georgian shoplifters and burglars in Europe can be confirmed.

5 Conclusion

The hierarchy and elements of Eurasian organised crime evolved over times. Different details and factors contributed to the establishment and progression of a criminal subculture such as thieves-in-law. Push factors in countries of origin and pull factors within European states favoured the fact that mobile organised criminal groups are highly active in high-volume property crimes. The challenges of this criminal phenomenon became a significant concern for the German (and European) public and police. To counter the phenomenon, Germany initiated a multi-agency cooperation to jointly inhibit the activities of Georgian organised crime groups and to shed light on the different layers and levels of the phenomenon. Hence, the feedback and results achieved so far have provided important guidance in the areas of focus for a continued evolution of the project. Therefore, the project is useful to fight Eurasian organised crime structures, but may also be suitable for future crime suppression efforts of other criminal phenomena.

References

BMI (2015). Polizeiliche Kriminalstatistik 2014. Berlin: Bundesministerium des Innern.

Cohen, D. S. (2011, July 25). Remarks by Under Secretary for Terrorism and Financial Intelligence David S. Cohen on the Presidential Strategy to Combat Transnational Organized Crime [Press release]. Retrieved from US Department of Treasury: http://www.treasury.gov/press-center/press releases/Pages/tg1256.aspx.

Fedpol (2010). Organisierte Kriminalität – Die "Diebe im Gesetz" – Ein Forschungsbericht [Organized Crime – The Thieves-in-law – A Research Paper]. Bern: Bundeskriminalpolizei BKP.

Focus (2015, June 11). Mit dieser Asyl-Masche schleusen sich Diebesbanden aus Georgien in Deutschland ein [This asylum – stitch up gangs of thieves from Georgia smuggle into Germany]. Focus Online. Retrieved from http://www.focus.de/politik/deutschland/dramatischer-anstieg-mit-dieser-asyl-masche-schleusen-sich-diebesbanden-aus-georgien-in-deutschland-ein_id_4742808.html.

Frisby, T. (1998). The Rise of Organized Crime in Russia: Its Roots and Social Significance. Europe-Asian Studies, 50, No. 1, 27–49: http://dx.doi.org/10.1080/09668139808412522.

Kattge, L. (2014). Russisch Eurasische OK am Beispiel der "Diebe im Gesetz" [Russian Eurasian OC using the example of "thieves in law"]. Kriminalistik, 3, 196–200.

Kegö, W., & Molcean, A. (2011). Russian Speaking Organized Crime Groups in the EU. Stockholm: Institute for Security and Development Policy.

Lungren, D. E. (1996). Russian Organized Crime. Retrieved from http://www.fas.org/irp/world/para/docs/rusorg3.htm.

Mayr, S. (2012, June 05). Bayerns bester Mafia-Jäger [Bavaria's best chaser of the Mafia]. *Süddeutsche Zeitung*. Retrieved from http://www.sueddeutsche.de/bayern/kampf-gegen-organisierte-kriminalitaet-bayerns-bester-mafia-jaeger-1.1375410.

Oxford Analytica (2010). Georgia/Europe: Coordinated police action deters OC. New York: Alacra Store.

Rahr, A., & Pachomow, P. (1998, November). Die Geschichte der russischen Kriminalität [The History of Russian Criminality]. Retrieved from http://www.kanka.de/aurora/konf4/mafia3.htm.

Slade, G. (2012a). No Country for Made Men: The Decline of the Mafia in Post-Soviet Georgia. Law & Society Review, 46, Number 3, 623–649: http://dx.doi.org/10.1111/j.1540-5893.2012.00508.x.

Slade, G. (2013). Reorganizing Crime – Mafia and Anti-Mafia in Post-Soviet Georgia. Oxford: Oxford University Press.

Varese, F. (1998). The Society of the Vory-v-Zakone, 1930s–1950s. Cahiers du monde russe: Russie, Empire russe, Union soviétique, États indépendants, 39, No. 4, 515–538: http://dx.doi.org/10.3406/cmr.1998.2538.

Webster, W. H. (1997). *Russian Organized Crime*. Retrieved from http://www.russianlaw.org/roc_csis.pdf.

Wiermer, C. (2015, April 28). Immer mehr Einbrüche: So gefährlich ist die Georgien-Mafia. [An increasing number of break-ins: How dangerous is the Georgia-Mafia]. *Hamburger Morgenpost*. Retrieved from http://www.mopo.de/politik—wirtschaft/jeder-zweite-in-asylverfahren-immer-mehr-einbrueche–so-gefaehrlich-ist-die-georgien-mafia,5066858,30548454.html.

Deutscher Teil
Part V

EU-Projekt „Research Network on Organised Crime" 2010–2016[1]

Die Zusammenarbeit auf internationaler, insbesondere auf europäischer Ebene im Bereich der Sicherheit gewinnt immer mehr an Bedeutung – das gilt auch für den Bereich der Polizeiforschung. Darauf basierend entstand im BKA die Idee, die europaweite Zusammenarbeit zwischen Wissenschaftlern und Praktikern aus Strafverfolgungsbehörden zur Bekämpfung der Organisierten Kriminalität (OK) zu fördern und ein Forum für den internationalen Austausch zwischen den beteiligten Akteuren zu schaffen. Gemeinsam mit Forschungsstellen aus dem Vereinigten Königreich, den Niederlanden und Schweden wurde das „OK-Forschungsnetzwerk" gegründet, dessen Aktivitäten von 2010 bis Ende Februar 2016 von der EU finanziell gefördert wurden.

1   EU-Projekt „Research Network on Organised Crime"

Das EU-Projekt „Research Network on Organised Crime" (März 2010 bis Februar 2013) wurde vom Bundeskriminalamt zusammen mit Forschungsinstitutionen aus dem Ausland im Rahmen des Programms der *Internal Security* (ISEC) „Prevention of and Fight against Crime" – Framework Partnerships beantragt. Ab 2010 wurde das Projekt von der EU zu 70 Prozent kofinanziert. Es beinhaltete zwei Arbeitstreffen der Projektpartner pro Jahr, die Ausrichtung einer jährlichen OK-Forschungskonferenz sowie die Veröffentlichung zweier Sammelbände mit Referentenbeiträgen der Forschungskonferenzen. Ziele des Projekts waren die Identifizierung aktueller Forschungsthemen und Untersuchungsmethoden zur OK-Forschung sowie der Informationsaustausch zu Forschungsprogrammen und Forschungsprojekten. Im Rahmen regelmäßiger Netzwerktreffen sollten Kriminalitätsfelder der OK beleuchtet und ausgewählte Themenschwerpunkte diskutiert werden. Die Forschungskonferenzen sollten einen Überblick über Forschungssituation und -schwerpunkte sowie Erkenntnisse über Kriminalitätslage und Bekämpfungsstrategien in europäischen Ländern liefern. Insgesamt wurde mit dem Projekt die Intensivierung des Austauschs mit nationalen und internationalen Akteuren aus Wissenschaft und Strafverfolgung im Bereich der Organisierten Kriminalität angestrebt.

---

[1]   Teile der Zusammenfassung wurden aus dem Artikel „Research Network on Organised Crime 2010–2013 – Bericht über ein EU-Projekt" von Ursula Töttel und Gerhard Flach, veröffentlicht in der deutschen Fachzeitschrift „Kriminalistik", Ausgabe 6/2014, übernommen.

Im Rahmen des ISEC-Programms „Prevention of and Fight against Crime 2007–2013, Action Grants 2011, General call for proposals" wurde ein EU-Folgeprojekt beantragt. Die Europäische Kommission hat erneut die Bedeutung des Netzwerks und der Forschungskonferenzen anerkannt und den Förderantrag genehmigt. Gegenüber dem ursprünglichen Projekt sind im Nachfolgeprojekt u. a. Änderungen hinsichtlich der (größeren) Teilnehmerzahl, der Referentengewinnung – auch außerhalb des EU-Raums – und der inhaltlichen Ausrichtung der jährlichen Forschungskonferenzen vorgenommen worden. Das beantragte Folgeprojekt „Research Network on Organised Crime 2013–2016" wurde seitens der EU gar zu 89,5 % finanziert und von März 2013 bis Ende Februar 2016 realisiert.

2 Entstehung der Projektidee

2.1 Suche nach Kooperationspartnern

Vor dem Hintergrund der zunehmend grenzüberschreitend agierenden OK-Gruppierungen wurde die Notwendigkeit gesehen, nicht nur die Bekämpfung, sondern auch die Forschung international auszurichten. Konkretisiert wurde diese Idee im Jahr 2007. Damals wurden erste Kontakte zur Realisierung des Vorhabens von Vertretern der „Forschungs- und Beratungsstelle für Organisierte Kriminalität und Wirtschaftskriminalität" des BKA mit dem *Home Office* in London geknüpft. Dem schloss sich ein erster Informationsaustausch zu OK-Forschungsprojekten in London an. 2008 kam es zu weiteren Kontaktaufnahmen zu möglichen Partnern in Belgien und den Niederlanden. Für die Auswahl der Institute war entscheidend, ob dort sozialwissenschaftliche Forschung zum Themenbereich OK betrieben wird. Eine Zusammenarbeit mit staatlichen Stellen wurde angestrebt. Bei näherer Betrachtung stellte sich heraus, dass das BKA in Bezug auf die kriminalistisch-kriminologische Forschung in Europa eine Sonderrolle spielt. Vergleichbare staatliche Forschungseinrichtungen sind zumeist bei Ministerien – und nicht unmittelbar in der Polizei – angegliedert, sodass mögliche Partnerinstitute außerhalb von Polizeibehörden gesucht wurden.

2.2 Gründung eines OK-Forschungsnetzwerks

Als Ergebnis der Kontaktgespräche fanden sich Ende 2008 die „Crime Research Development Unit" des Home Office London, das „Research and Documentation Centre" (WODC) des Justizministeriums Den Haag und die niederländische Polizeiakademie Apeldoorn zusammen, um das OK-For-

schungsnetzwerk zu gründen. Auf Anregung aus den Niederlanden wurde festgelegt, die Teilnehmerzahl des Netzwerks möglichst überschaubar zu halten, um bestmögliche Effizienz zu gewährleisten. Im Jahr 2010 erfolgten wichtige Änderungen: Die Polizeiakademie schied aus dem Netzwerk aus und die dem schwedischen Justizministerium untergeordnete Forschungsstelle „Swedish National Council for Crime Prevention" (Brå), Stockholm, trat dem Netzwerk bei. Die Mitglieder der schwedischen Forschungsstelle konnten aufgrund des späteren Beitritts keine EU-Förderung beantragen. Seit dieser Zeit hat sich die Zusammensetzung des Netzwerks nicht mehr verändert.

Die erste OK-Forschungskonferenz fand im November 2008 in Frankfurt am Main statt. Zu diesem Zeitpunkt war offen, ob weitere Konferenzen folgen und das Netzwerk Bestand haben würde.

3   Forschungskonferenzen und Netzwerktreffen

3.1   Teilnehmer und Ausrichtung der Konferenzen

In den Jahren 2008 bis 2015 veranstaltete das Bundeskriminalamt in Frankfurt am Main, Wiesbaden, Niedernhausen und Mainz acht internationale OK-Forschungskonferenzen. Die Tagungen ermöglichten einen umfassenden Überblick über die Situation der OK-Forschung und -Bekämpfung in zahlreichen europäischen Ländern. Sie boten ein Forum für den grenzübergreifenden Gedanken- und Informationsaustausch von Wissenschaftlern und Polizeipraktikern zu Themen und Fragestellungen, wie beispielsweise bereits praktizierten und denkbaren alternativen Feldzugängen bei empirischen Forschungsprojekten und praktische Umsetzung wissenschaftlicher Erkenntnisse. Sie gaben aber auch Einblicke in Strategien der Polizei sowie Besonderheiten und Schwierigkeiten der Strafverfolgung. Wissenschaftler und Experten der Strafverfolgungsbehörden aus Albanien, Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, dem Vereinigten Königreich, Italien, Kroatien, den Niederlanden, Norwegen, Österreich, Polen, Tschechien, Schweden, der Schweiz, Slowenien, Spanien, der Türkei, Ungarn und den USA stellten ihre Forschungsaktivitäten oder die jeweilige nationale Kriminalitäts- und Bekämpfungssituation auf den Konferenzen vor. Auch Vertreter von Europol und Interpol waren beteiligt.

Die Konferenzen waren nach geografischen Gesichtspunkten ausgerichtet. Themenbereiche waren OK-Forschung und -Lage in den Nachbarstaaten Deutschlands (2008), in Südosteuropa (2009), Südwesteuropa (2010), Westeuropa (Vereinigtes Königreich, Niederlande, 2011) und Nordeuropa (2012). Die Konferenzen von 2013 bis 2015 waren phänomenologisch ausgerichtet.

Themen waren Organisierte Kriminalität und Internet (2013), die verschiedenen Gesichter der Organisierten Kriminalität (2014) und internationale OK-Gruppierungen (2015).

Auf den jeweils zweitägigen Konferenzen stellten je sieben bis acht Referenten die besonderen Situationen in ihren Ländern bzw. ausgewählte Aspekte aus eigener Perspektive vor. Die Referentenauswahl war eine gemeinsame Leistung der Partnerinstitutionen des Netzwerks.

3.2 Ziele der Netzwerktreffen

Das OK-Forschungsnetzwerk dient der Intensivierung des direkten Kontakts zwischen behördlichen Forschungsinstituten und ermöglicht eine abgestimmte Bewertung von Entwicklungstrends in Wissenschaft und Strafverfolgung. Neben den anlassbezogenen Kontakten auf Arbeitsebene fanden im Rahmen der Netzwerkaktivitäten pro Jahr zwei Treffen der beteiligten Institute statt, die auch den gemeinsamen Vorbereitungen der OK-Forschungskonferenzen dienten. Ein Austausch zu laufenden und geplanten Forschungsprojekten, aber auch darüber hinausgehender Erkenntnisse – z. B. aus Bedrohungsanalysen, Lageeinschätzungen und Bekämpfungsansätzen – sowie von Informationen aus oder über Fachtagungen oder sonstige relevante Veranstaltungen und Ereignisse fand statt.

4 Projektdurchführung

4.1 Zusammenarbeit mit den Projektpartnern

Bei der Durchführung des Projekts zeigte sich, dass eine realistische Zeitplanung sowie die vorherige Festlegung der Verantwortlichkeiten und Aufgaben im Rahmen des gemeinsamen Vorhabens sinnvoll und hilfreich sein würden. Aus den anfänglichen Treffen und Absprachen mit noch ausgeprägt formellem Charakter und zunächst konzentriert auf das Gelingen des EU-Projekts entwickelte sich eine vertrauensvolle und unkomplizierte Zusammenarbeit unter den Partnerinstitutionen über die Umsetzung der Projektaktivitäten hinaus.

Notwendigerweise ergriff das BKA als projektleitende Institution in jedem Fall die Initiative für die geplanten Aktivitäten. Auch erleichterte es die Koordination, die in Besprechungen vereinbarten Arbeitspakete und sonstigen Vereinbarungen schriftlich festzuhalten. Um einen Informationsaustausch unter

den Netzwerkpartnern außerhalb der zweijährlich stattfindenden Treffen herzustellen, haben sich Telefonschaltkonferenzen bewährt. Als vorteilhaft erwies sich die Kontinuität der personellen Zusammensetzung des Netzwerks.

Nicht unterschätzt werden dürfen die Fülle von „Kleinarbeit" bei der Vorbereitung einer Konferenz und der Veröffentlichung einer Buchpublikation sowie der bei allen Projektaktivitäten erforderliche Abstimmungsprozess mit Forschungseinrichtungen aus den drei anderen europäischen Staaten.

4.2   Erfahrungen und Ergebnisse aus der Projektarbeit

An dieser Stelle sei unterstrichen, dass die Unterstützung durch das BKA-interne Referat „EU-geförderte Projekte" der Abteilung „Internationale Koordinierung" von großem Vorteil für den gesamten Prozess war. Von dort wird Hilfestellung bei der Beantragung und Durchführung von EU-Projekten geleistet und dem Projektdurchführenden ein „Financial Manager"[2] für jedes im Rahmen des ISEC-Programms durchgeführte Projekt zur Seite gestellt.

Im Verlauf des Projekts wurden Kontakte zu nationalen und europäischen Universitäten, Hochschulen der Polizei und anderen Instituten, die Forschung zu Organisierter Kriminalität betreiben, aufgebaut. Auf den Konferenzen haben Vertreter von Forschungseinrichtungen, Polizeibehörden, Staatsanwaltschaften und internationalen Organisationen Vorträge gehalten. Für die inhaltliche Ausgestaltung der einzelnen Treffen wurden stets Anregungen und Themenvorschläge aus dem Teilnehmerkreis aufgenommen und unter den Netzwerkpartnern für die Planung nachfolgender Veranstaltungen diskutiert.

Die Veröffentlichungen gewähren einen Überblick über die Forschungssituation in anderen europäischen Ländern und sind wie die Abstracts der Referate über die BKA-Homepage zugänglich.[3] Die erste Buchpublikation „Research Conferences on Organised Crime at the Bundeskriminalamt in Germany 2008–2010" wurde im Oktober 2011 veröffentlicht.[4] Die zweite Veröffent-

---

[2] Der „Financial Manager" ist für das Management der Finanzen gegenüber der Europäischen Kommission zuständig. Dazu gehören die Budgetierung, die Definition geeigneter Kostenstrukturen und die Verrechnung von Serviceleistungen.

[3] Informationen zu den OK-Forschungskonferenzen stehen zur Verfügung unter http://www.bka.de/DE/ThemenABisZ/Forschung/OK-Forschungskonferenzen/ok-forschungskonferenzen__node.html?__nnn=true sowie in englischer Sprache unter http://www.bka.de/nn_195376/EN/SubjectsAZ/Research/OrganisedCrimeResearch/organisedCrimeResearch__node.html?__nnn=true.

[4] Töttel, Ursula/Büchler, Heinz (2011): Research Conferences on Organised Crime at the Bundeskriminalamt in Germany 2008–2010, Polizei + Forschung Band 43, unter: http://www.bka.de/nn_193482/DE/Publikationen/Publikationsreihen/01PolizeiUndForschung/01PolizeiUndForschung__node.html?__nnn=true.

lichung über die Konferenzen von 2009 bis 2012 erschien im September 2013.[5] Darüber hinaus wurden gemeinsame Beiträge der Mitglieder des OK-Forschungsnetzwerks veröffentlicht.[6]

In Zusammenarbeit mit zwei Forschungseinrichtungen aus dem Netzwerk wurde im März 2013 ein internationales Forschungsprojekt zum Thema „Organisierte Kriminalität und Cybercrime" initiiert und ein Antrag zur Förderung im Rahmen des ISEC-General-Calls der EU-Kommission gestellt, der im Dezember 2013 bewilligt worden ist. Das zweijährige Projekt „Cyber-OC – Scope and manifestations in selected EU member states" lief von April 2014 bis März 2016.

5   Weitere Fördermöglichkeit der Aktivitäten

Für den Bereich der Inneren Sicherheit gab es bisher sechs Förderinstrumente der Europäischen Kommission. Diese wurden zum 01. 01. 2014 auf zwei Instrumente reduziert, und zwar auf den Asyl- und Migrationsfonds (AMF) und den Innere-Sicherheit-Fonds (ISF) 2014–2020,[7] sodass auch das ISEC-Programm, im Rahmen dessen das hier beschriebene EU-Projekt gefördert worden war, durch den ISF abgelöst wird.

Zurzeit gibt es keinen entsprechenden Call der Europäischen Kommission, um ein weiteres Folgeprojekt nahtlos zu beantragen, möglicherweise bieten aber zukünftige Ausschreibungen geeignete Voraussetzungen dafür.

---

[5] Töttel, Ursula/Bulanova-Hristova, Gergana/Büchler, Heinz (2013): Research Conferences on Organised Crime at the Bundeskriminalamt in Germany (Vol. II) – Organised Crime – Research and Practice in Western and Northern Europe, 2011–2012, Polizei + Forschung Band 45, unter: http://www.bka.de/nn_193482/DE/Publikationen/Publikationsreihen/01PolizeiUnd-Forschung/01PolizeiUndForschung__node.html?__nnn=true.

[6] Mehrere Artikel zum Themenbereich Menschenhandel sind 2011 veröffentlicht worden in: Trends in Organized Crime: Special Issue: Human Trafficking, Vol. 14, 2011, http://www.springerlink.com/content/1084-4791/14/2-3/ (Link zu den frei zugänglichen Artikeln). Ein Konferenzbericht zur 4. OK-Forschungskonferenz im November 2011 wurde im Jahr 2012 publiziert: Töttel, Ursula/Bulanova-Hristova, Gergana/Kleemans, Edward (2012): Trends in Organised Crime, Vol. 15, Research on organized crime in Western Europe – 4th research conference „OC research in Western European states", in Wiesbaden, http://link.springer.com/article/10.1007/s12117-012-9176-y#page-1.

[7] Siehe auch Europäische Kommission unter: http://ec.europa.eu/dgs/home-affairs/financing/fundings/funding-home-affairs-beyond-2013/index_en.htm.

6   Fazit

Die Durchführung des EU-Projekts „Research Network on Organised Crime"
erbrachte sowohl fachlich als auch persönlich einen Mehrwert für die Betei-
ligten am OK-Forschungsnetzwerk. Zum einen konnten aktuelles Wissen
über Entwicklungen und Forschungsaktivitäten sowie Erkenntnisse aus der
Strafverfolgung zum Thema „Organisierte Kriminalität" ausgetauscht wer-
den, zum anderen hat sich durch die Treffen der Mitarbeiter der jeweiligen
Forschungseinrichtungen über mehrere Jahre die Zusammenarbeit verfestigt.
Auch die Teilnehmer an den OK-Fachkonferenzen konnten von dem Erfah-
rungsaustausch im Rahmen der Vorträge und den Kontakten profitieren. Über
die Veröffentlichungen wurden die Ergebnisse der Tagungen einem breiten
Fachpublikum zugänglich gemacht. Es wird angestrebt, das OK-Forschungs-
netzwerk aufrechtzuerhalten und auch künftig Fachkonferenzen auszurichten.

Beschreibung der Partnerinstitute

Forschungs- und Beratungsstelle für Organisierte Kriminalität, Wirtschaftskriminalität und Kriminalprävention, Bundeskriminalamt (BKA), Deutschland

Die Forschungs- und Beratungsstelle für Organisierte Kriminalität, Wirtschaftskriminalität und Kriminalprävention ist als Teil der „Kriminalistisch-kriminologischen Forschungsgruppe"[1] des BKA die führende Forschungsinstitution zum Thema „Organisierte Kriminalität" bei der deutschen Polizei. Dort sind folgende Forschungsstellen angesiedelt:

– Forschungs- und Beratungsstelle Terrorismus/Extremismus (FTE),

– Forschungs- und Beratungsstelle Polizeiliche Kriminalstatistik (PKS), Dunkelfeldforschung,

– Operative Fallanalyse (OFA), Forschungs- und Beratungsstelle für Gewalt- und Jugendkriminalität,

– Forschungs- und Beratungsstelle für Organisierte Kriminalität, Wirtschaftskriminalität und Kriminalprävention,

– Beratungsstelle für polizeipraktische Rechtsfragen und Rechtspolitik,

– Forschungs- und Beratungsstelle für Cybercrime.

Gemäß § 2 des Gesetzes für das Bundeskriminalamt (BKAG) obliegt es der Kriminalistisch-kriminologischen Forschungsgruppe, die Polizeien des Bundes und der Länder zu unterstützen, polizeiliche Methoden und Arbeitsweisen sowie phänomenologische Fragestellungen der Kriminalitätsbekämpfung zu erforschen und zu beantworten. Das Team der Forschungsstelle für OK, Wirtschaftskriminalität und Kriminalprävention ist interdisziplinär zusammengesetzt und besteht aus Polizeipraktikern und Wissenschaftlern, die an der Schnittstelle zwischen Wissenschaft und Praxis unter Anwendung wissen-

---

[1] Beim BKA ist für 2016 eine Umorganisation geplant, von der auch die Kriminalistisch-kriminologische Forschungsgruppe betroffen sein wird. Zwar wird sie weiterhin bestehen, jedoch nicht in der im Text beschriebenen Organisationsform und in anderer Anbindung.

schaftlicher Methodik an der Beantwortung polizeilicher Fragen sowie der (Weiter-)Entwicklung von Lösungskonzepten arbeiten. Hierbei wird Wert auf eine enge Abstimmung mit den Anwendern bzw. Bedarfsträgern gelegt. Es werden Forschungs- und Beratungsaufgaben auf den Feldern der Organisierten Kriminalität, des Menschenhandels und der Schleusungskriminalität, der Wirtschafts- und Finanzkriminalität sowie der Kriminalprävention wahrgenommen.

Folgende Themen bilden derzeit Schwerpunkte der Arbeit, zu denen 2015 Forschungsprojekte abgeschlossen wurden bzw. aktuell Projekte durchgeführt werden:

– Im Oktober 2015 wurde die Studie „Compliance-Systeme und ihre Auswirkungen auf die Verfolgung und Verhütung von Straftaten der Wirtschaftskriminalität und Korruption" veröffentlicht. Sie ist das Resultat einer empirischen Untersuchung, in der der Frage nachgegangen wurde, inwieweit Compliance-Systeme Auswirkungen auf die Aufgabenerledigung der Strafverfolgungsbehörden in Fällen von Wirtschaftskriminalität und Korruption sowie die Kommunikation zwischen Unternehmen und Strafverfolgungsbehörden haben.

– Ebenfalls im Oktober 2015 wurden die Ergebnisse einer im Bundeskriminalamt realisierten Sekundäranalyse zum Thema „Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes" publiziert.

– Beim derzeit laufenden Projekt „Arzneimittelkriminalität 2" (AMK2) werden Situationsanalysen durchgeführt sowie Defizite bei der Kriminalitätsbekämpfung im Bereich der Arzneimittelkriminalität identifiziert sowie Handlungsempfehlungen zur Behebung dieser Defizite formuliert. Es ist ein Nachfolgeprojekt des 2007 vom BKA veröffentlichten Projekts „Arzneimittelkriminalität – ein Wachstumsmarkt". Die Studie wird voraussichtlich 2016 abgeschlossen.

– Des Weiteren wird gemeinsam mit den Projektpartnern Research and Documentation Centre (WODC) in Den Haag und Swedish National Council for Crime Prevention (Brå) in Stockholm das EU-finanzierte Projekt *„Cyber OC – Scope and manifestations in selected EU member states"* durchgeführt, das voraussichtlich am 01.04.2016 abgeschlossen sein wird.

Die Forschungsstelle unterstützt zudem als assoziierter Partner eine Reihe laufender Projekte im Rahmen der nationalen Sicherheitsforschung. Es handelt sich um nachfolgende Verbundprojekte zu Themen der Organisierten

Kriminalität und Wirtschaftskriminalität, gefördert durch das deutsche Bundesministerium für Bildung und Forschung (BMBF):[2]

– Auswirkungen der Liberalisierung des Internethandels in Europa auf den Phänomenbereich der Arzneimittelkriminalität (ALPhA),

– Prävention und Intervention bei Menschenhandel zum Zweck sexueller Ausbeutung – Eine multidisziplinäre und institutionsübergreifende Perspektive (PrIMsA),

– Prävention von Kapitalmarktdelikten und Risiken der Geldwäsche (PKG),

– Risikomanagement der Korruption aus der Perspektive von Unternehmen, Kommunen und Polizei (RIKO),

– Verfahren zur Erhellung des Dunkelfelds als Grundlage für Kriminalitätsbekämpfung und -prävention am Beispiel antiker Kulturgüter (Illicid),

– Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa (WISKOS).

---

[2] Ein Überblick über die laufenden Forschungsprojekte aus dem Programm „Forschung für die zivile Sicherheit" findet sich auf der Homepage des VDI-Technologiezentrums: http://www.vditz.de/forschungsfoerderung/sicherheitsforschung/laufende-forschungsprojekte-im-ueberblick/.

Die Gruppe *Organised and Cyber Crime Research & Analysis* (Forschungs- und Analysegruppe für Organisierte Kriminalität und Cybercrime, OCCRA) ist ein im britischen Innenministerium (*Home Office*) tätiges Forscherteam aus Sozialwissenschaftlern, Operationsforschern und Wirtschaftswissenschaftlern. Das Innenministerium ist das federführende Ministerium für Einwanderung und Passwesen, Drogenpolitik, Kriminalität, Terrorismusbekämpfung und Polizei. OCCRA führt objektive Analysen durch und unterstützt damit Entwicklung, Umsetzung, Überwachung und Auswertung staatlicher Politik und Leistungen.

Das Forscherteam hat die Aufgabe, für das *Strategic Centre for Organised Crime* (Strategisches Zentrum für Organisierte Kriminalität) des Home Office analytische Unterstützung zu leisten, und will:

– Kenntnisse erweitern und wichtige Beweislücken im Bereich der schweren und Organisierten Kriminalität sowie Cybercrime schließen,

– eine evidenzbasierte Politikgestaltung unterstützen und

– einen Beitrag zur Bearbeitung der in der *Serious and Organised Crime Strategy*[1] (Strategie gegen schwere und Organisierte Kriminalität) und der *UK Cyber Security Strategy*[2] (Cyber-Sicherheitsstrategie des Vereinigten Königreichs) benannten Zielstellungen leisten, um die Widerstandsfähigkeit des Vereinigten Königreichs gegen schwere und Organisierte Kriminalität sowie Cyberangriffe zu erhöhen.

In der Praxis bedeutet dies Durchführung und Vergabe quantitativer und qualitativer Forschungsprojekte, Bewertung und Synthese von Nachweisen aus einer Reihe von Quellen, Beratung und Informationen zu einer großen Anfragenpalette von Ministern und politischen Beamten sowie eine Schnittstellen-

---

[1] *Serious and Organised Crime Strategy* (2013), abrufbar unter: https://www.gov.uk/government/publications/serious-organised-crime-strategy.

[2] *The UK Cyber Security Strategy* (2011), abrufbar unter: https://www.gov.uk/government/publications/cyber-security-strategy.

funktion zwischen politischer und wissenschaftlicher Forschung zu Kriminalität und Polizeiarbeit.

Das OCCRA-Forschungsprogramm wird im Grundsatz bestimmt durch die in der *Serious and Organised Crime Strategy 2013* (Strategie gegen schwere und Organisierte Kriminalität 2013) beschlossenen Vereinbarungen. Die Veröffentlichung dieser Strategie fiel zusammen mit dem Arbeitsbeginn der *National Crime Agency* (Nationale Kriminalitätsagentur, NCA) und will den Umfang der das Vereinigte Königreich und dessen Interessen schädigenden schweren und Organisierten Kriminalität reduzieren. Basierend auf der zur Terrorismusbekämpfung entwickelten Strategie wurden vier Ziele formuliert:

– Strafverfolgung und Störung/Beeinträchtigung an schwerer und Organisierter Kriminalität beteiligter Personen (*Pursue* – Verfolgung),

– Verhinderung einer Beteiligung an derartigen Aktivitäten (*Prevent* – Prävention),

– Intensivierung des Schutzes gegen schwere und Organisierte Kriminalität (*Protect* – Schutz) und

– Minderung der Auswirkungen dieser Kriminalität dort, wo sie stattfindet (*Prepare* – Vorbereitung).

Zu den kürzlich publizierten Arbeiten des OCCRA zählen ein Bericht über die kriminellen Laufbahnen von OK-Straftätern,[3] eine Prüfung der Forschungsergebnisse zu Organisierter Kriminalität,[4] eine Schätzung des Umfangs und der Kosten schwerer und Organisierter Kriminalität[5] und ein Bericht über die Art von Onlinestraftaten.[6] Aktuelle Analyseprojekte konzentrieren sich auf die Untersuchung der Märkte für illegale Güter, die Auswirkungen von Cybercrime auf den Ruf von Unternehmen, die Effektivität von Störungstaktiken gegen Cybercrime, den Umfang der Verurteilungen von OK-Gruppen sowie die wirtschaftliche Bewertung diverser neuer Initiativen und Maßnahmen.

---

[3] *Understanding Criminal Careers in Organised Crime* (2013), abrufbar unter: https://www.gov.uk/government/publications/understanding-criminal-careers-in-organised-crime.

[4] *Cyber Crime: A Review of the Evidence* (2013), abrufbar unter: https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence.

[5] *Understanding Organised Crime: Estimating the Scale and the Social and Economic Costs* (2013), abrufbar unter: https://www.gov.uk/government/publications/understanding-organised-crime-estimating-the-scale-and-the-social-and-economic-costs.

[6] *The Nature of Online Offending* (2015), abrufbar unter: https://www.gov.uk/government/publications/the-nature-of-online-offending.

Forschungsstelle für Kriminalität, Strafverfolgung und Sanktion (*Crime, Law Enforcement and Sanctions Research Division***) des *Research and Documentation Centre* (Forschungs- und Dokumentationszentrum, WODC) beim Ministerium für Sicherheit und Justiz der Niederlande**

Das WODC ist ein zum Ministerium für Sicherheit und Justiz der Niederlande gehörendes halbautonomes Forschungs- und Wissenszentrum, das für dieses Ministerium sowie für dessen untergeordnete Stellen arbeitet. Das WODC betreibt Forschung auf den Gebieten Sozial-, Verhaltens- und Rechtswissenschaft. Ziel des Instituts ist die Schaffung von Wissen über aktuelle und zukünftige für die Sicherheit und Justiz relevante Phänomene. Dazu gehören Bewertungen politischer Richtlinien und Programme sowie Prognosemodelle. Das WODC macht das gewonnene Wissen einer breiten Öffentlichkeit zugänglich. Alle Forschungsergebnisse werden auf der eigenen Website zur Verfügung gestellt. Forschungsprojekte zu wichtigen Kernbereichen und umfassenden Themen werden auch in Buchform oder elektronisch veröffentlicht. Darüber hinaus berät das WODC das Ministerium für Sicherheit und Justiz auf der Basis seiner Forschungsergebnisse. Letztlich fungiert das WODC auch als Vergabestelle, da ein beträchtlicher Teil des Forschungsportfolios externen Partnern zugewiesen wird. Das WODC setzt sich aus folgenden Abteilungen zusammen:

– Forschungsabteilung Kriminalität, Strafverfolgung und Sanktionen,

– Forschungsabteilung Justizverwaltung, Gesetzgebung, internationale und Ausländerangelegenheiten,

– Abteilung Forschungsauftragsvergabe,

– Abteilung Statistische Daten und Analyse politischer Richtlinien,

– Abteilung Dokumentation und Information.

Die *Crime, Law Enforcement and Sanctions Research Division* (Forschungsstelle für Kriminalität, Strafverfolgung und Sanktion) hat etwa 30 bis 35 Mitarbeiter und arbeitet zu einer Vielzahl von Themen. Wesentliche Forschungsschwerpunkte konzentrieren sich auf OK und Wirtschaftskriminalität, Terrorismus, Cybercrime, strafrechtliche Ermittlungsmethoden, Rückfallkriminalität sowie neurobiologische Faktoren kriminellen Verhaltens. WODC arbeitet mit wichtigen externen Forschungsinstituten wie beispielsweise dem

Centre for Information and Research on Organised Crime (Zentrum für OK-Information und -Forschung, CIROC), einer Kooperation zwischen WODC und der Freien Universität Amsterdam, der Erasmus-Universität Rotterdam, der Universität Utrecht und der Universität Maastricht, sowie dem *Research Network on Organised and Economic Crime* (Forschungsnetzwerk zu OK und Wirtschaftskriminalität).

Dutch Organised Crime Monitor

Ein wichtiges laufendes Forschungsprojekt ist der *Dutch Organised Crime Monitor* (Niederländischer OK-Monitor). Die Hauptquellen dieses Forschungsprojekts sind die abgeschlossenen Ermittlungsakten der niederländischen Polizei zu kriminellen Gruppen. In vier Suchdurchläufen (Datensweeps) des Zeitraums 1996–2012 wurden 150 umfangreiche Ermittlungen systematisch analysiert. Jeder Fall konzentriert sich auf ein kriminelles Netzwerk. Zusammen enthalten die 150 Fallberichte Informationen zu vielen Hundert Verdächtigen. Derzeit läuft der fünfte Datensweep, mit dem die Datenbank um 30 neue Fallstudien erweitert wird. Nach dieser fünften Runde wird der *Dutch Organised Crime Monitor* einen beträchtlichen Querschnitt von 180 Fällen umfassen, die unterschiedliche Straftaten wie die diversen Formen von Drogenhandel/-produktion, Cybercrime, Schleusung, Menschenhandel und illegalem Waffenhandel, aber auch (groß angelegte) Betrugsfälle und Geldwäsche abdecken.

Jede Fallstudie beginnt mit strukturierten Interviews mit Polizeibeamten und/oder Staatsanwälten. Nach diesen Interviews werden die polizeilichen Akten analysiert und zusammengefasst. Sie enthalten die Ergebnisse der gesamten Polizeiarbeit, wie beispielsweise Abhörmaßnahmen, Observationstechniken, Undercover-Polizeiarbeit, Intelligence-Sammlung, Vernehmungen und vorgenommene finanzielle Ermittlungen. Diese Quellen liefern einen detaillierten Einblick in die soziale Welt der Organisierten Kriminalität. Bei der Beschreibung und Analyse der polizeilichen Akten wird eine umfangreiche Checkliste mit Details zu folgenden Leitfragen eingesetzt: Wie ist die Zusammensetzung der Gruppe und wie kooperieren die Straftäter? Welche Arten illegaler Aktivitäten führen sie durch und wie operieren sie? Wie interagieren sie mit den Chancen und Risiken ihres Umfelds? Welche Einnahmen erzielen sie mit ihren Straftaten und wie setzen sie diese Einnahmen ein? Neben den Polizeiakten werden auch Interviews mit Fachleuten, Informationen aus anderen Ermittlungen, vertrauliche Berichte, Kriminalitätsanalysen sowie die (wissenschaftliche) Literatur genutzt. Die Fallstudien des *Dutch Organised Crime Monitor* wurden verwendet, um vier umfangreiche Berichte über das Wesen der Organisierten Kriminalität in den Niederlanden für das niederländische Parlament sowie zahlreiche wissenschaftliche Artikel zu verfassen.

Schwedischer Nationaler Beirat zur Kriminalitätsprävention

Der Schwedische Nationale Beirat zur Kriminalitätsprävention (*Brottsföre-byggganderadet* – Brå), eine dem Justizministerium untergeordnete Behörde, ist ein Forschungs- und Entwicklungszentrum innerhalb des Geschäftsbereichs des Justizministeriums. Die Tätigkeit von Brå besteht hauptsächlich in der Kriminalitätsbekämpfung und der Erhöhung der Sicherheit in der Gesellschaft durch die Erfassung von Daten und die Verbreitung von Wissen über Kriminalität und Präventionsarbeit. Der Rat erstellt die offizielle Kriminalitätsstatistik Schwedens, evaluiert Reformen, forscht und bietet Unterstützung für die Präventionsarbeit vor Ort. Die Forschungsergebnisse von Brå dienen den Entscheidungsträgern des Justizsystems, des Parlaments und der Regierung als Wissensgrundlage für die Verabschiedung und Umsetzung von Gesetzen und politischen Richtlinien. Brå arbeitet regelmäßig mit Organisationen und Anstalten des öffentlichen Rechts zusammen. Das Institut richtet außerdem im Auftrag der schwedischen Regierung das kriminologische Symposium in Stockholm, eine jährlich stattfindende internationale Forschungskonferenz, aus. Brå wird von einem Generaldirektor geleitet, der von der Regierung ernannt wird.

Forschungsstelle für Wirtschafts- und Organisierte Kriminalität

Die Forschungsstelle für Wirtschafts- und Organisierte Kriminalität nimmt eine nationale Expertenfunktion im Bereich von Wirtschafts- und Organisierter Kriminalität ein. Umweltkriminalität und Straftaten im Zusammenhang mit dem kulturellen Erbe gehören ebenfalls zu ihren Forschungsthemen. Die Forschungsstelle führt verschiedene Forschungsprojekte durch, häufig in Zusammenarbeit mit anderen Akteuren und unter Verwendung externer Mittel, und sie verbreitet diese Forschung auf verschiedenen Wegen. Die Forschungsprojekte beleuchten die Beschaffenheit der Wirtschafts- und Organisierten Kriminalität, vorwiegend in Schweden, wobei ein besonderes Augenmerk auf die Methoden und Strategien für die Kriminalitätsprävention gerichtet ist. Über die Forschungsarbeit hinaus nehmen die Vertreter der Forschungsstelle regelmäßig an Arbeitsgruppen teil und übernehmen sich daraus ergebende Aufgaben. An der Spitze der Forschungsstelle steht ein Abteilungsleiter.

Forschungsstrategie

Die Forschungsstelle für Wirtschaftskriminalität und Organisierte Kriminalität konzentriert sich in erster Linie auf neue und bisher unerforschte Formen von Straftaten und Gemeinschaftsmaßnahmen gegen derartige Kriminalität. In den vergangenen Jahren hat sie Berichte zu verschiedenen Themen wie Erpressung, Korruption und sonstigen Formen rechtswidriger Einflussnahme, Geldwäsche, dem Finanzmanagement des Drogenhandels, organisiertem Steuerbetrug, Sozialversicherungsbetrug, in kulturellen Traditionen begründeten Straftaten, Umweltkriminalität, Spielmanipulationen, Beschlagnahme illegal erworbener Vermögenswerte, administrativen und behördenübergreifenden Vorgehensweisen zur OK-Bekämpfung und Geldwäsche publiziert.

Frühere und aktuelle Projekte

2015 gab die Forschungsstelle einen Bericht mit Ermittlungen heraus, wie falsche Identitäten und andere gefälschte Urkunden eingesetzt werden, um unterschiedliche Betrugsdeliktarten zu begehen. Sie publizierte außerdem einen Bericht über die Struktur von Spielmanipulationen in Schweden sowie einen Bericht über Versicherungsbetrug.

Die *Division of Economic and Organised Crime Research* arbeitet derzeit an folgenden Projekten:

– rechtswidrige Einflussnahme auf Staatsbeamte,

– rechtswidrige Einflussnahme auf die Migrationsagentur,

– Fallstudie der behördenübergreifenden Vorgehensweise gegen organisierte Kriminalität in der Kommune Södertälje,

– ARIEL – *Assessing the Risk of the Infiltration of Organized Crime in EU MSs Legitimate Economies: a Pilot Project in 5 EU Countries* (ARIEL – Bewertung des Risikos der OK-Infiltration in die legale Wirtschaft: ein Pilotprojekt in fünf EU-Ländern)

Rechtswidrige Einflussnahme auf Staatsbeamte

Seit 2005 hat Brå diverse Formen rechtswidriger Einflussnahme untersucht, d. h. Belästigungen, Bedrohungen, Vandalismus, Gewalt und Korruption gegen Staatsbeamte als Zeugen und Kläger. Von Brå wurde zu diesem Thema

eine Serie von Berichten herausgegeben (z. B. 2005: 8, 2008: 8, 2009: 7, 2012: 12 und 2014: 4). Darin behandelte Themen betreffen beispielsweise Hochrisiko-Beamtengruppen für rechtswidrige Einflussnahme, die überwiegenden Situationen für rechtswidrige Einflussnahme und Beispiele für Parteien, die rechtswidrige Einflussnahme praktizieren, und die von ihnen genutzten Methoden. In den Berichten wurden auch Mittel zur Prävention und Abwehr von Korruptionsversuchen präsentiert. Derzeit liegen keine aktualisierten Studien zum Umfang der rechtswidrigen Einflussnahme auf Staatsbeamte vor. Daher wird der *Swedish National Council for Crime Prevention* die 2005 erstellte Studie/Umfrage erneut durchführen.

Rechtswidrige Einflussnahme auf die Migrationsagentur

Bei der *Migration Agency* (Migrationsagentur) handelt es sich um die Behörde, die die gesellschaftliche Migrations- und Asylpolitik – ein bisweilen kontroverses Thema – umsetzt. Beamte der Behörde sind wie zu erwarten unterschiedlichen Formen rechtswidriger Einflussnahme ausgesetzt, die in engen Kundenbeziehungen stattfinden kann. Die Beschlüsse der Agentur sind für die Zukunft der Betroffenen oft von entscheidender Bedeutung. Die Studie will die Einflussnahme und den Druck abbilden, dem die *Migration Agency* und ihre Mitarbeiter ausgesetzt sind. Dafür müssen geeignete Politiken und Praktiken zur Prävention und Bekämpfung formuliert werden. Zu den zu beantwortenden Fragen zählen: In welchem Zusammenhang findet versuchte Einflussnahme statt? Welche Folgen hat dies? Welche Art der rechtswidrigen Einflussnahme hat die größte Wirkung? Wie kann man künftige Versuche verhindern? Die dazu eingesetzten Methoden sind Interviews, Fokusgruppen, Observationen der Beteiligten und Seminare. Die *Migration Agency* braucht Kenntnisse über rechtswidrige Einflussnahme. Eine detaillierte Studie zu diesem Bereich erhöht den Kenntnisstand zum Thema sowohl bei der Behörde als auch in der Gesamtgesellschaft.

Fallstudie der behördenübergreifenden Vorgehensweise gegen Organisierte Kriminalität in der Kommune Södertälje

In der Fallstudie von Södertälje wird die behördenübergreifende Vorgehensweise gegen Organisierte Kriminalität mithilfe teilnehmender Beobachtungen, Interviews und Auswertungen von Ermittlungsakten untersucht. Das Projekt ist einzigartig, weil es in Echtzeit die behördenübergreifende Initiative verfolgt und damit eine detaillierte Analyse ermöglicht, wie sich die Kooperation zwischen den beteiligten Behörden entwickelt. Die Studie ist ein Ableger einer größeren Auswertung der nationalen behördenübergreifenden Initia-

tive zur OK-Bekämpfung in Schweden und wird in Zusammenarbeit von Brå und Stockholmer Bezirkspolizei bzw. regionaler Kriminalpolizei durchgeführt.

ARIEL – Bewertung des Risikos der OK-Infiltration in die legale Wirtschaft: ein Pilotprojekt in fünf EU-Ländern

Ein weiteres OK-Projekt ist ARIEL – *Assessing the Risk of the Infiltration of Organized Crime in EU MSs Legitimate Economies: a Pilot Project in five EU Countries* (Bewertung des Risikos der OK-Infiltration in die legale Wirtschaft: ein Pilotprojekt in fünf EU-Ländern), ein von der EU finanziertes Projekt, das Brå zusammen mit Transcrime (Italien, als Koordinatoren), der Universität Durham (Vereinigtes Königreich), dem *Netherlands Institute for the Study of Crime and Law Enforcement* (Niederländisches Institut zur Erforschung von Kriminalität und Strafverfolgung) und der *Faculty of Criminal Justice and Security* (Fakultät für Strafrecht und Sicherheit) der Universität Maribor (Slowenien) realisiert. Das Projekt identifiziert Methoden diverser OK-Gruppen, um legale Unternehmen zu infiltrieren, zu kontrollieren und zu leiten. Ein besonderer Schwerpunkt gilt der Identifizierung von Risikofaktoren, um künftige Infiltrationen zu verhüten. Das empirische Material besteht aus Intelligence-Daten, Ermittlungen und Seminaren mit Fachleuten staatlicher Behörden und Sicherheitspersonal aus der Privatwirtschaft.

Organisierte Kriminalität und das Internet: 6. Forschungskonferenz Organisierte Kriminalität in Niedernhausen, 2013

Vom 25. bis 26. September 2013 fand die 6. OK-Forschungskonferenz in Niedernhausen bei Wiesbaden statt. Das Thema der Tagung lautete „Organised Crime and the Internet". Auf dieser Konferenz wurde ein Einblick in den aktuellen Forschungsstand und Bekämpfungsstrategien insbesondere im Hinblick auf bestehende Verbindungen zwischen OK und Cybercrime gegeben. Sie lieferte Erkenntnisse zum Aufbau krimineller Gruppen, die das Internet und dessen Kommunikationsmöglichkeiten zur Begehung von Straftaten nutzen. Relevante „Cyber-OK-Fälle" und Informationen zum Organisationsgrad von Tätergruppierungen wurden präsentiert, Besonderheiten bei Ermittlungsverfahren und rechtliche Rahmenbedingungen dargestellt und Fragestellungen der Strafverfolgung sowie künftiger Forschungsbedarf diskutiert. Verglichen mit den bisherigen Forschungskonferenzen haben anteilmäßig mehr Experten der Strafverfolgungsbehörden als Wissenschaftler ihre Erkenntnisse präsentiert, augenscheinlich da sich die sozialwissenschaftliche Forschung bis dahin nur begrenzt mit dem Thema „Cyber-OK" auseinandergesetzt hatte.

Zu dieser Konferenz werden keine Vorträge veröffentlicht, da es sich bei Cybercrime um einen sich schnell verändernden Phänomenbereich handelt und die Vortragsinhalte von 2013 bei Publizierung dieses Bands im Jahr 2016 kaum mehr aktuell sein dürften. Nachfolgend seien die Beiträge aber zusammengefasst dargestellt.

James Pang, Assistant Director des *Global Complex for Innovation* (IGCI) bei Interpol Singapur, stellte in seinem Vortrag **„Organised Crime in the Digital Age"** die Aktivitäten Interpols im Bereich Cybercrime vor. Der *Global Complex for Innovation* ist ein modernes Forschungs- und Entwicklungszentrum zur Identifizierung von Straftaten und Straftätern, für innovative Ausbildung, operative Unterstützung und internationale Partnerschaften in Singapur.[1] Im Bereich Cybercrime hat der IGCI die Aufgabe, die 190 Mitgliedsländer bei Cyberattacken und länderübergreifenden Ermittlungsverfahren zu unterstützen. Dies beinhaltet u. a. auch, ein globales Netz mit rund um die Uhr erreichbaren Ansprechpartnern für Cybercrime und Datenbankdienste bereitzustellen, aufkommende neue Bedrohungen zu erkennen und an die Mitgliedsländer zu kommunizieren. Cybercrime gehört zu den am schnellsten wachsenden Kriminalitätsbereichen. Immer mehr Kriminelle nutzen die Ge-

---

[1] Siehe http://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation/About-the-IGCI.

schwindigkeit, die Bequemlichkeit und die Anonymität moderner Kommunikationstechnologie, um eine große Bandbreite krimineller Delikte zu begehen. Die Kosten von Cybercrime werden weltweit auf 110 Milliarden USD geschätzt. Die jährliche Anzahl der Opfer beträgt 556 Millionen, d. h. 18 Opfer pro Sekunde. Interpol veranstaltet in gewissen Abständen Arbeitstreffen zur Informationstechnologie, um die Entwicklung von Strategien, Technologien und Informationen zu den neuesten IT-Kriminalitätsmethoden zu verbessern. Zur Veranschaulichung dieser Aktivitäten stellte Pang einige internationale mit Unterstützung Interpols realisierte Operationen vor: Beim „Singapore Internet Banking"-Betrugsfall verschaffte sich ein Cyberring mittels auf dem digitalen Schwarzmarkt gekaufter Malware Zugang zu Bankdaten. Die betrügerisch erlangten Geldbeträge wurden nach Tadschikistan transferiert. Die IP-Adressen der Anwerber der Geldkuriere führten in das Vereinigte Königreich.

Beim Fall „Unlimited Operations" wurden während zweier Aktionen, die jeweils weniger als 24 Stunden andauerten, weltweit in 26 Ländern 20.000 finanzielle Transaktionen durchgeführt. Dabei wurden von der RAKBANK im Dezember 2012 5 Millionen USD und im Februar 2013 von der Bank of Muscat 40 Millionen USD transferiert. In einem Fall von Arzneimittelkriminalität wurden mehr als 13.700 Websites mit illegalen Arzneimitteln geschlossen. Insgesamt wurden 10,1 Millionen möglicherweise gesundheitsgefährdende Medikamente im Wert von 36 Millionen USD sichergestellt. Im Rahmen der Operation SOGA IV zu illegalen Fußballwetten während der Europameisterschaft zwischen Mai und Juli 2012 wurden bei einer von Interpol koordinierten Operation gegen Glücksspielnetzwerke in Asien fast 300 Personen festgenommen. An der Operation nahmen Strafverfolgungsbehörden aus China, inklusive Hongkong und Macau, Malaysia, Singapur, Indonesien und Vietnam teil. Es wurden mehr als 200 polizeiliche Razzien in Spielkasinos durchgeführt. Im Rahmen der Operation SOGA IV wurde eine Reihe internationaler Treffen mit den Interpol-Zentralbüros der beteiligten Staaten einschließlich der „Asia Pacific Expert Group on Organized Crime" und Workshops durchgeführt. Die letzte SOGA-Operation hat gezeigt, dass durch nationale und internationale Polizeikooperationen illegale Glücksspielnetzwerke erfolgreich bekämpft werden können. Die verschiedenen SOGA-Operationen haben zu mehr als 7000 Festnahmen und zur Schließung von Onlinecasinos, die Wetten im Wert von 85 Mio. USD organisiert hatten, und zur Beschlagnahme von 27 Mio. USD Bargeld geführt. Das Angebot illegaler Glücksspiele im Internet ist in den letzten Jahren stark gestiegen. Banken und Kreditkartenunternehmen sind mittlerweile alarmiert und weisen die Strafverfolgungsbehörden auf verdächtige Transaktionen hin. Die Polizei kontaktiert Internetprovider, um auf Websites mit illegalen Wettspielen aufmerksam zu machen.

„Organised Cybercrime – overview from a Swedish perspective" war das Thema der Präsentation von **Ulrika Sundling**, Detective Superintendent bei der Cybercrime-Einheit des *National Bureau of Investigation* (NBI) in Stockholm. In ihrem Vortrag gewährte sie einen Überblick über die Zuständigkeiten ihrer Behörde und deren Schwierigkeiten bei der Bekämpfung von Cybercrime.

Sundling präsentierte eine Übersicht über die Organisation des *National Bureau of Investigation*, das Teil des *National Police Board* (Nationale Polizeidirektion) beim schwedischen Justizministerium ist. Den Auftrag des NBI kann man in vier Teile untergliedern: organisierte Schwerkriminalität, mobile Organisierte Kriminalität, internationale Kooperation sowie Krisenmanagement. Das NBI bekämpft organisierte schwere Straftaten auf sowohl nationaler als auch internationaler Ebene und soll kriminellen Organisationen in Schweden entgegenwirken. Einer der vier Bereiche des NBI ist die *Criminal Intelligence & Investigation Division* (Abteilung für polizeiliche Analyse und Ermittlungen), die Informationen zu schweren Straftaten und Organisierter Kriminalität erhebt, verarbeitet und analysiert. Ihre Arbeit konzentriert sich auf Rauschgiftkriminalität, illegale Einwanderung, Menschenhandel, Geldwäsche, Umweltstraftaten, Kinderpornografie, Cybercrime, Tötungsdelikte und Organisierte Kriminalität. Die ihr unterstellte *IT Crime Unit* analysiert Informationen und sichert Beweismaterial bei polizeilichen Operationen und Ermittlungen, die eine spezielle IT-Kompetenz erfordern. Sie greift auf Spezialisten für Internetermittlungen, IT-Forensik und Kinderpornografie zurück. In Schweden nimmt die Organisierte Kriminalität seit dem Jahre 2000 zu. Aufgrund der stärkeren Nutzung des Internets steigen auch die Fälle von Computerkriminalität an. Rauschgifthandel in jeder Form ist ein Kriminalitätsbereich der Organisierten Kriminalität. Der Rauschgiftschmuggel nach Schweden wird von gut organisierten kriminellen Netzwerken beherrscht und es gibt keine Anzeichen für einen Rückgang von Drogenversorgung und -missbrauch. Sowohl Menschenhandel als auch -schleusung werden normalerweise von homogenen kriminellen Netzen organisiert. Der Schmuggel von Zigaretten und Alkohol ist ein lukratives Geschäft und scheint immer attraktiver zu werden. Die Wirtschaftskriminalität intensiviert sich ebenfalls und die Fälle, bei denen sich legale und illegale Aktivitäten überschneiden, nehmen zu. Legale Teilnehmer können ebenso wie Straftäter Teil krimineller Machenschaften sein. Eine der gewichtigsten Bedrohungen im Internet sind Botnets, also Netzwerke infizierter Computer, die von einem Angreifer gesteuert werden. Sundling stellte den Fall „Case DDoS" vor, weil es 2009 massive DDoS-Angriffe gegeben hat und diese Botnets auch zu Betrugszwecken genutzt wurden. Auch wurden mit OK in Zusammenhang stehende „Money Mules" (Finanzagenten) entdeckt. Der Fall zeigte, dass Botnets auf unterschiedlichste Weise genutzt werden, weil ein OK-Zusammenhang bestand und hinter den

Attacken ein großes kriminelles Netzwerk steckte. Bei Onlinebankdiensten gehört ein Banktrojaner zu den aggressivsten Cyberbedrohungen. Fast jeder Banktrojaner setzt eine Attacke durch „einen Mann im Browser" ein, mit dem die Angreifer Schadcodes direkt in die Browser der Opfer einschleusen, sich für sie ausgeben und Zugriff auf ihre Bankkonten bekommen. Anhand des Falls „Banktrojaner" zeigte Sundling, dass ein umfangreiches OK-Netzwerk verantwortlich war. In Untergrundforen bieten kriminelle Syndikate „Crime as a Service" (Straftat als Service, CaaS) an, also illegale Dienstleistungen wie die Infizierung großer Computerzahlen, den Versand von Spam und selbst Angriffe vom Typ „Direct Denial of Service" (Direkte Leistungsverhinderung, DDoS). Die Herausforderungen für die schwedische Polizei bestehen darin, häufig komplexe Ermittlungen gegen Untergrundforen zu führen und sich mit der Anonymität der Computerkriminalität und Datenverschlüsselung auseinanderzusetzen, was durch Anonymisierungsdienste weiter erschwert wird.

In seinem Vortrag **„Onlinebanking-related ID-theft – a case study revealing Cybercrime-related OC"** gab der Erste Kriminalhauptkommissar **Mirko Manske** aus dem Bereich „Lage und Analyse Cybercrime" beim Bundeskriminalamt einen Überblick über die Entwicklungen im Bereich des Cyberbetrugs im Onlinebanking.

Das sogenannte „Phishing im Zusammenhang mit Onlinebanking" ist wohl die bekannteste Variante des digitalen Identitätsdiebstahls. Für das Jahr 2013 wurden dem Bundeskriminalamt 4.096 Sachverhalte bekannt. Phishing bildet im Hinblick auf die vorhandenen Möglichkeiten und die zu erzielenden Gewinne weiterhin ein lukratives Betätigungsfeld für die Täterseite. So betrug die durchschnittliche Schadenssumme des „Phishings im Zusammenhang mit Onlinebanking" auch im Jahr 2013 rund 4.000 Euro pro Fall. Nachdem durch verschiedene Schutzmaßnahmen wie u. a. die Nutzung des mTAN-Verfahrens im Onlinebanking sowie eine noch intensivere Sensibilisierung der Anwender eine annähernde Halbierung der Fallzahlen im Jahr 2012 hatte erreicht werden können, zeigte sich für das Jahr 2013 wieder ein merklicher Anstieg. Hauptgrund dürfte sein, dass sich die Täterseite den veränderten Rahmenbedingungen technisch angepasst und neue oder verbesserte Schadsoftware entwickelt hat, um die Sicherheitsmaßnahmen zu umgehen. Manske quantifizierte die angezeigten Fälle im Phishing im Zusammenhang mit Onlinebanking von 2005 bis 2012 und verdeutlichte ihren ständigen Anstieg, aber auch den zeitweisen Rückgang nach Einführung von Sicherheitsmaßnahmen wie des i-TAN-Verfahrens. Diesen Zahlen stellte er die vom BKA geschätzten tatsächlichen Fälle gegenüber, da bei Weitem nicht alle Fälle angezeigt werden. Manske stellte verschiedene Fälle vor, um die Vorgehensweisen der Onlinebetrüger darzustellen. Beim Fall „Dinosaur-Phish" wurden 2006 Kunden mithilfe einer Spammail auf eine gefälschte Bankseite gelockt und mit dem Hin-

weis auf neuer Sicherheitsmaßnahmen gebeten, einen Link zu benutzen und TAN-Nummern sowie Zugangsdaten anzugeben. Nach Einführung des i-TAN-Verfahrens ab 2008 etablierte sich eine andere Vorgehensweise: die Vektorattacke „Man in the Middle". Der Kunde erhielt eine E-Mail mit einer Malware im Anhang. Beim Öffnen des Anhangs wurde ein Trojaner auf dem Computer des Kunden installiert. Wenn sich der Kunde nun unter Nennung der Kennwörter in das Onlinebankingsystem einloggte, änderte der Trojaner Empfänger und zu überweisenden Betrag. Die Bank verlangte im Anschluss eine i-TAN zur Bestätigung der Überweisung. Der Kunde legitimierte damit die betrügerische Geldüberweisung. Bei dieser „Man in the Middle"-Attacke steht der Angreifer entweder physikalisch oder logisch zwischen den beiden Kommunikationspartnern und kontrolliert mit seinem System den Datenverkehr zwischen den Kommunikationspartnern. Dabei kann er die Informationen einsehen und manipulieren. Die steigende Verbreitung mobiler Endgeräte wie Smartphones sowie die teilweise immer noch mangelnde Sensibilität der Nutzer hinsichtlich digitaler Gefahren im Umgang mit diesen mobilen Endgeräten sorgten für eine weiterhin hohe Attraktivität für die Täterseite. Dies zeigte sich u. a. auch in der Zunahme für Betriebssysteme mobiler Endgeräte programmierte Schadprogramme. Von 2006 bis 2010 wurden für das Phishing im Onlinebanking häufig sogenannte „Money Mules" rekrutiert, um betrügerische Transaktionen durchzuführen. Die Rekrutierung erfolgte durch sogenannte Phishing-Shops. Etwa von 2010 bis 2012 dominierte das Geschäftsmodell der kriminellen Infrastrukturdienste: Mehrere Infrastrukturanbieter kooperieren oder stehen zeitgleich auf einem globalen Markt im Wettbewerb um ihre spezialisierten Dienste, beispielsweise Geldkurierdienste. 2012 tauchte die Vektorattacke ZitMO (*Zeus in the Mobile*) auf. Bei dieser Vorgehensweise manipulierte die auf dem Rechner mittels eines Trojaners infizierte Malware die Kommunikation innerhalb des Webbrowsers, wobei andere als die vom Nutzer vorgegebenen Informationen weitergegeben wurden. Das Smartphone des Opfers wurde mit durch einen per SMS gesandten Trojaner mit Malware infiziert. Sobald sich das Opfer mit seinen Zugangsdaten in das Bankportal einloggte, schalteten sich die Betrüger mithilfe des *Zeus*-Trojaners in das Bankgeschäft ein und forderten das Opfer mittels Pop-ups auf, die Art des Smartphones und die Anschlussnummer mitzuteilen. Bei diesem Vorgang wurde das Gerät infiziert. Mithilfe des Trojaners wurden die Daten an einen *Command & Control Server* weitergeleitet. Der Server der Täter generierte eine Textnachricht mit der Weisung, ein Update des Smartphones durchzuführen. Die Textnachricht enthielt einen WAP-Link zu einer infizierten Website. Eine andere Vorgehensweise war der Verkauf bereits infizierter Smartphones z. B. über eBay. Ab 2013 tauchten sogenannte „Runner" zur Abhebung der Geldsummen an Geldautomaten auf, die zwischen den kriminellen Gruppen für spezielle Dienste gehandelt und ausgetauscht wurden.

Edwin Kruisbergen, Wissenschaftlicher Mitarbeiter am *Research and Documentation Centre* des Niederländischen Ministeriums für Sicherheit und Justiz, hielt eine Präsentation mit dem Titel **„Digitized organised crime: traditional organised crime and ICT"**.

Traditionelle Organisierte Kriminalität umfasst Rauschgifthandel, Schleusung, Menschenhandel, illegalen Waffenhandel und Geldwäsche sowie andere kriminelle Aktivitäten. Edwin Kruisbergen konzentrierte sich auf Rauschgifthandel. Im ersten Teil seiner Präsentation führte er aus, wie die Informations- und Kommunikationstechnologie (ICT) in den Bereichen Logistik, Kommunikation, Sozialkapital und Geldwäsche eingesetzt werden kann. Am Beispiel der Logistik führte Kruisbergen Strafrechtsfälle aus der jüngsten Vergangenheit an, um zu illustrieren, wie Täter die ICT für Rauschgiftproduktion, -verteilung (Verkauf) und -schmuggel nutzen. Zur *Drogenproduktion* werden via Internet Ausgangsstoffe wie GBL (Gamma-Butyrolacton), das zur Herstellung von GHB (Gamma-Hydroxybuttersäure = flüssiges Ecstacy) eingesetzt wird, beschafft. Personen aus den Niederlanden haben Tausende Liter GBL aus China importiert und über das Internet verkauft. „Niederländisches" GBL wurde in vielen Ländern von Deutschland bis China sichergestellt. In anderen Fällen haben die an der Produktion synthetischer Drogen beteiligten Täter das Internet genutzt, um Maschinen zur Herstellung von Tabletten zu kaufen. Außerdem werden mehrere Schwarzmärkte im tiefen Web genutzt, um Drogen zu *vertreiben*. Beispiele für diese Schwarzmärkte sind die Silk Road, Black Market Reloaded und Atlantis. Ein weiterer wichtiger Aspekt der Drogenkriminalität sind *Transport und Schmuggel*. Einige Monate vor der Forschungskonferenz wurden in einem einmaligen Fall „digitalen" Drogenschmuggels neun Personen verhaftet, Hunderte Kilogramm Kokain sowie 100 Kilogramm Heroin und mehr als 1 Million € Bargeld beschlagnahmt. Die Täter nutzten die ICT zur Durchführung von Drogenschmuggel über den Hafen Antwerpen: Sie hackten das Computernetz von Containerterminals und Reedereien. Dadurch konnten die Täter Entladezeit und -ort der Container manipulieren, in denen ihre Mittäter Rauschgift versteckt hatten.

Gründliche empirische Forschung zur Nutzung der Informations- und Kommunikationstechnologie in der traditionellen Organisierten Kriminalität ist selten. Im zweiten Teil seiner Präsentation befasste sich Kruisbergen daher mit wichtigen Forschungsfragen im Zusammenhang mit ICT und Organisierter Kriminalität. Grundsätzlich zu fragen ist, wie weit verbreitet und entwickelt die ICT-Nutzung tatsächlich ist. Weitere Fragen lauten: Wie nutzen an OK-Straftaten beteiligte Täter die ICT? Welche Folgen hat die ICT-Nutzung für andere Aspekte einer OK-Gruppe? Verändert die Nutzung der modernen Kommunikationstechnologien die Art und Weise, wie kriminelle Gruppen organisiert sind? Unterstützt die ICT Täter dabei, spezielle Engpässe in ihrem Modus Operandi zu beseitigen? Führt die ICT-Nutzung unter Umständen zu

neuen Engpässen? Hat die ICT-Nutzung Folgen für die Märkte und die Ebenen, auf denen eine Gruppe tätig ist? Im Zusammenhang mit normalen legalen Unternehmen wird häufig geäußert, dass das Internet *ein* oder vielleicht *der* wichtigste Antrieb für Globalisierung ist. Gilt das auch für kriminelle Unternehmungen? Andere Fragen beziehen sich auf die Täter selbst: Nutzen die „üblichen Verdächtigen" die neue Technologie oder geht die neue Technologie mit einem neuen Tätertypus einher?

Wenn empirische Fragen wie diese und andere beantwortet sind, können eher theoretische Fragen adressiert werden. Letztendlich lautet nach Kruisbergen die wichtigste Frage: Wenn die traditionelle OK (teilweise) digital wird, sollte das Auswirkungen auf unser OK-Verständnis haben? Mit anderen Worten: Haben theoretische Einsichten und Konzepte, die beispielsweise zur sozialen Einbettung Organisierter Kriminalität bei offline tätigen Straftätergruppen entwickelt wurden, weiter Gültigkeit, wenn man den Modus Operandi der digitalen OK betrachtet? Ein solches Konzept ist die *soziale Einbettung* Organisierter Kriminalität. Von besonderer Bedeutung für Täter in der Organisierten Kriminalität ist das Sozialkapital. Um an OK-Aktivitäten beteiligt und erfolgreich zu sein, muss man die richtigen Personen kennen: Käufer, Verkäufer, Produzenten, Transporteure, Co-Finanziers, Geldwäscher usw. Weil die meisten Straftäter keine Werbung treiben, müssen sie sich auf ihre Sozialbeziehungen stützen, d. h. fähige und zuverlässige Täter in ihrem sozialen Netzwerk finden. Man könnte fragen, ob die „Bekanntschaft zu den richtigen Personen" sich so verändert, dass „man sich im Deep Web auskennen muss". Wird das Internet die Bedeutung von Sozialkompetenz verringern? Die Beantwortung solcher Fragen ist eine ehrgeizige Aufgabe. Kruisbergen argumentierte, dass deren Beantwortung aber notwendig ist, wenn wir wirklich verstehen wollen, wie die Informations- und Kommunikationstechnologie die Organisierte Kriminalität verändert.

Dr. Melvin Soudijn, Senior Researcher im *High Tech Crime Team* der niederländischen Nationalpolizei in Zoetermeer, referierte in seinem Vortrag **„Offender Convergence Settings in Cyberspace" (Täterräume im Cyberspace)** über die Ergebnisse der Auswertung eines Internetforums.

Der Begriff *Offender Convergence Settings* (OCS) wurde 2003 erstmalig von Marcus Felson (Texas State University) benutzt, um physische Treffpunkte für mutmaßliche Täter im Zusammenhang mit Straftaten zu beschreiben. Dort treffe man sich mit Freunden, lerne neue Leute kennen, tausche Informationen aus, verkaufe gestohlenes Material oder plane neue kriminelle Aktivitäten. OCS liefere Struktur und Kontinuität für den Einzelnen und das Netzwerk. Soudijn analysierte in seinem Projekt, ob diese OCS auch im Cyberspace existieren. Bisherige Analysen haben gezeigt, dass sich Cyberkriminelle im virtuellen Raum u. a. in sogenannten *Carding*-Foren treffen. Mit

Carding bezeichnet man die missbräuchliche Nutzung persönlichen Bank- und Kreditkartendaten. Einige der Foren sind für jeden offen, der an dieser Art krimineller Aktivitäten interessiert ist, während andere Foren streng abgeschottet sind.

Eines dieser Carding-Foren wurde bei polizeilichen Ermittlungen der KLPD im Jahr 2008 offengelegt. Obwohl das Forum für Personen ohne Zugang blockiert war, bestand aufgrund eines technischen Fehlers die Möglichkeit, eine digitale Kopie anzufertigen. Dies verschaffte der Polizei einen außerordentlichen Einblick in die kriminellen Aktivitäten von Cyberkriminellen. Soudijn führte eine Textanalyse von fast 154.000 Postings von über 1.800 Mitgliedern des Carding-Forums aus den Jahren 2003 bis 2008 durch. Die Datenerfassung erfolgte im Rahmen einer *Social Network Analysis* (SNA). Die realen Identitäten der Mitglieder wurden nicht erfasst, lediglich die Nicknames wurden bekannt. Das Carding-Forum hatte zwei Funktionen: einen Raum für den Austausch von Informationen (*knowledge place function*) und einen Raum, in dem Produkte und Dienstleistungen angeboten und gesucht werden können (*market place function*), zur Verfügung zu stellen. Im Durchschnitt standen die Forumsmitglieder mit 16 Personen in Verbindung. Neue Mitglieder bauten in kürzester Zeit mehrere Verbindungen auf. Auch kamen diverse kriminelle Gruppen miteinander in Kontakt. Einige handelten mit gestohlenen Kreditkarten oder Malware, andere führten Geldtransfers durch, wieder andere waren in das Grafikdesign für die Erstellung falscher Websites oder als zwischengeschaltete Stelle für die Vermittlung anonymer Server zuständig. Die Realisierung krimineller Aktivitäten wurde nicht im Forum abgesprochen. Die Forumsverwalter bemühten sich, vertrauenswürdige Mitglieder anzuwerben. Sie bauten ein System von Garantien, Peer Review und Status auf. Um ein Mitglied des Forums zu werden, wurde ein Betrag von USD 50,00 fällig. Dafür wurden ein Username und ein Passwort ausgegeben. Für einen Zugang zum gesamten Forum mussten zwei Forumsmitglieder als Referenzpersonen genannt werden. Ein Peer-Review-System diente der Bewertung der angebotenen Waren und Dienstleistungen sowie der Vertrauenswürdigkeit. Zudem wurde den Forumsmitgliedern ein Status als Moderator, Newcomer, Service, Member, Verified Member, Administrator, Deer (Forumsregeln gebrochen), Unresolved Problems oder Ripper (andere Forumsmitglieder betrogen) zugewiesen. Anhand der Textanalyse konnten folgende vier Phasen des Cardings herausgearbeitet werden: 1. Vorbereitung, 2. Durchführung des Diebstahls von Bank- oder Kreditkarten, 3. „Money Mule"-Phase, in der das Geld durch einen Geldkurier transferiert wird, und 4. *Cashing*-Phase, bei der das betrügerisch erbeutete Geld zum Hauptverdächtigen gelangt. Die Auswertung der Kommunikation im Carding-Forum zeigte auch, dass das Hacking von Bankaccounts oder das Erlangen betrügerischen Gelds nicht die eigentliche

Schwierigkeit der Cyberkriminellen ist. Vielmehr besteht das Problem darin, keine Spuren zu hinterlassen, wenn das Geld auf andere Konten transferiert wird. Soudijn erklärte, dass es für die Strafverfolgung nicht einfach sei, Zugang zu kriminellen Foren zu bekommen. Sie befänden sich auf Servern, für die keine geografischen Grenzen existieren. Im Rahmen des Projekts der niederländischen KLPD seien zumindest einige Einblicke gewonnen worden.[2]

In ihrem Vortrag **„In the meantime in cyber space …"** sprach **Floor Jansen**, Beraterin beim *Team High Tech Crime* der *Dutch National Police Services Agency* in Driebergen über einen Fall internationaler Kinderpornografie und die Schwierigkeiten der Strafverfolgungsbehörden, anonyme Seiten im Internet aufzudecken.

Jansen beschrieb, dass Ende 2010 ein Foto eines zweijährigen Jungen mit einem Spielzeug im Internet entdeckt wurde. Das Opfer wurde von der niederländischen Polizei identifiziert. Ein Mann aus Amsterdam, der pornografisches Material von 84 Kindern besaß, wurde als Produzent der Pornografie-Website ermittelt. Er nutzte in erster Linie das soziale Netzwerk ICQ und baute Kontakte zu Kindern in 43 Ländern auf. 440 Chatlogs konnten sichergestellt und 1.116 Aliasnamen zugeordnet werden. Im Rahmen der Ermittlungen wurden 80 weitere Fälle bekannt. Das *Internet Relay Chat* (IRC), ein textbasiertes Chatlog, das Roundtables auf den Kanälen und zwischen zwei Teilnehmern (Anfragen) zulässt, wurde ebenfalls genutzt. Die Produzenten pornografischem Materials sind in erster Linie deshalb schwierig zu identifizieren, weil sie normalerweise nur Zugang zu Pornografie-Websites haben, um neues Material einzustellen. Die Ermittlungen führten zum anonymen TOR-Netzwerk, das auch als *The Onion Router* beschrieben wird; also ein System, bei dem Nutzer ihren Standort maskieren und anonym kommunizieren können. TOR ist Teil des *Deep Webs*, das in Suchmaschinen wie Google nicht indiziert wird. Mit dem Websitemonitoringtool DSRT wurde eine Netzwerkraupe entwickelt, um weitere relevante Websites zu ermitteln. Die niederländischen Beamten suchten systematisch nach allen identifizierten Websites und erstellten eine Liste der darunter auf Kinderpornografie spezialisierten. In TOR waren viele andere Straftäter aktiv. Insgesamt wurden 54 relevante Seiten mit einer Sammlung von 220.000 Fotos und Videos gefunden, 33 % des Materials waren unbekannt. Zehn illegale Websites wurden zerstört und mit dem Logo der niederländischen Polizei und folgendem Text gespammt: „Diese Seite ist Gegenstand strafrechtlicher Ermittlungen der niederländischen Nationalen Polizei. Sie sind nicht anonym. Wir wissen, wer sie

---

[2] Weitere Informationen in „Cybercrime and virtual offender convergence settings" von Melvin Soudijn und Birgit C. H. T. Zegers, veröffentlicht am 25. 05. 2012 in „Trends in Organized Crime": http://link.springer.com/article/10.1007%2Fs12117-012-9159-z#page-1.

sind. Die Produktion, der Vertrieb und der Besitz von Kinderpornografie sind Kapitalverbrechen. Alle bei diesen strafrechtlichen Ermittlungen gesammelten Informationen werden an die entsprechenden Behörden weitergeleitet." Eine dieser illegalen Websites bestand nur zwei Wochen. Die niederländische Polizei arbeitete mit dem FBI zusammen, das 2012 in den Vereinigten Staaten die „Operation Torpedo" startete. Mit einem Durchsuchungsbefehl des Gerichts Rotterdam begannen die US-Agenten, Websitestandorte zu ermitteln. Der Pornografie-Fall ist ein Beispiel für einen klassischen Kriminalfall mit digitaler Komponente. Die gesamte Operation offenbarte, wie internationale Behörden zusammenarbeiten können, und könnte eine Warnung für Straftäter sein, dass das Internet nicht so anonym ist, wie angenommen wird.

John T. Picarelli, PhD, Programmmanager für transnationale Angelegenheiten am *National Institute of Justice* (NIJ) des *U.S. Department of Justice*, gab in seinem Vortrag **„Cybercrime and Threat Convergence" (Cybercrime und Bedrohungsszenarien)** einen Überblick über die Bedrohung durch Cybercrime in den USA, stellte Verbindungen zur OK und zum Terrorismus her und schilderte die US-amerikanische Vorgehensweise zur Bekämpfung des Phänomens.

Das NIJ ist die Forschungs-, Entwicklungs- und Evaluationsbehörde des US-Justizministeriums, erforscht Kriminalitätsphänomene sowie Rechtsprobleme und befasst sich mit den Bereichen Sozialwissenschaften, Forensik und Technologie. Die Abteilung „Transnationale Angelegenheiten" unterhält weltweit Kontakte. NIJ erforscht die sogenannte „Threat convergence", das Zusammenwirken von zwei oder mehreren Bedrohungsszenarien und deren Einfluss auf illegale Märkte. Hierbei ist vor allem von Interesse, wie sich diese Bedrohungsszenarien auf illegale Märkte im Internet auswirken. Die Michigan State University hat die Entstehung neuer illegaler Märkte im Internet, konkret 13 Webforen, zehn in russischer und drei in englischer Sprache, untersucht, die als Umschlagplätze für gestohlene Kontodaten u. a. dienen. Es wurde festgestellt, dass 84 % der zum Verkauf angebotenen Daten gestohlen waren, 45 % davon Kreditkartendaten oder Kontoinformationen, wobei die Mehrzahl der Daten aus Europa stammte. Herausgearbeitet wurde auch, dass in den Onlinenetzwerken eine klare Arbeitsteilung besteht. Die zentralen Figuren sind die Verkäufer. Die Netzwerke sind unübersichtlich und es scheint eine Hierarchie zu fehlen. In den USA entstehen immer mehr Websites zur Prostitution und zum Menschenhandel, begünstigt durch die sozialen Medien wie Twitter, Facebook und YouTube. Die Organisation „Shared Hope International" lokalisierte über 5.000 Personen im Bereich des Frauenhandels. In sieben US-amerikanischen Städten wächst der Sexhandel im Internet seit den 90er-Jahren stetig. Dies gilt insbesondere für die Verbreitung illegaler Videos.

Terroristische Organisationen nutzen das Internet, um gewalttätige Extremisten zu rekrutieren und Angriffe vorzubereiten. Jedoch gibt es in den USA erst wenige Erkenntnisse zur Selbstrekrutierung oder Selbstradikalisierung über das Internet. Die Brandeis University im US-Bundesstaat Massachusetts hat wesentliche Erkenntnisse zur Rolle des Internet bei der Rekrutierung und Radikalisierung gewaltbereiter Extremisten in den USA, die al-Qaida, die Hisbollah und Hamas unterstützen, gewonnen. Radikalisierte Extremisten, die al-Qaida unterstützen, sind im Durchschnitt über zehn Jahre jünger als der Durchschnitt der Hisbollah- und Hamas-Unterstützer. Es wurde festgestellt, dass sich die Zeitspanne von der ersten Radikalisierung bis zur kriminellen Tat oder zur Festnahme von sechs Jahren vor 9/11 auf 1,7 Jahre nach 2007 verkürzt hat. Untersuchungen zum „Do it yourself"-Terrorismus haben gezeigt, dass radikalisierte Individuen Verhaltensregeln über Netzwerke online erhalten. 2013 hat ein Projekt zu den Einflussfaktoren bei der Radikalisierung mit Bezug zur transnationalen OK begonnen. Es sind Interviews mit 100 in den USA einsitzenden Unterstützern geplant. Dabei soll erhoben werden, welche Expertise Mitglieder in internationalen OK-Netzwerken benötigen und inwieweit diese legale Institutionen in ihre kriminellen Aktivitäten einbinden. Als sehr bedeutsam für die Bekämpfung von Cybercrime werden insofern gute Verbindungen zum privaten Sektor in Form von Public-private-Partnerships erachtet, als der private Sektor die Infrastruktur im Internet kontrolliert. Picarelli verwies auf die gute Kooperation im europäischen CIRCAMP-Projekt (*Cospol Internet Related Child Abusive Material Project*) zur Kinderpornografie. Mitglieder im Projekt sind 14 europäische Länder, unterstützt durch Europol und Interpol. CIRCAMP wird durch das „EC Safer Internet Programme" der Europäischen Kommission unterstützt, kooperiert aber weltweit mit betroffenen Staaten. Picarelli bekräftigte abschließend, dass im Bereich Cybercrime eine internationale Zusammenarbeit zwischen amerikanischen und europäischen Behörden erwünscht und notwendig ist.

In seinem Vortrag **„Transborder investigations in cybercrime cases – New challenges for law enforcement"** stellte **Rainer Franosch**, leitender Staatsanwalt der Zentralstelle zur Bekämpfung der Internetkriminalität bei der Generalstaatsanwaltschaft Frankfurt am Main, die Herausforderungen grenzüberschreitender Ermittlungen zur Cyberkriminalität vor.

Franosch veranschaulichte den steigenden Professionalismus von Cyberkriminellen, die die neuen Technologien zur Durchführung von Straftaten nutzen, und ging auf die Möglichkeiten der Strafverfolgungsbehörden im Zusammenhang mit Cyberkriminalität in Deutschland ein. Der Generalstaatsanwalt ist für Ermittlungsverfahren in Fällen von Terrorismus, Spionage, Hochverrat und Völkermord zuständig. Seit Juni 2011 existiert in Deutschland die Zentralstelle zur Bekämpfung der Internetkriminalität (CDCC) als bundesweit zuständige Staatsanwaltschaft in dringenden Cybercrime-Fällen.

Die von ihr bearbeiteten Verfahren sind oft international ausgerichtet; häufig werden sie in Zusammenarbeit mit dem US Secret Service und dem FBI durchgeführt. Mittlerweile unterhalten einige deutsche Bundesländer auf Internetkriminalität spezialisierte Abteilungen bei ihren Polizeibehörden und Staatsanwaltschaften. Jede Generalstaatsanwaltschaft der Bundesländer kann länderübergreifende Ermittlungsverfahren durchführen. Die grenzüberschreitende Erlangung elektronischer Beweismittel ist für die Strafverfolgungsbehörden eine große Herausforderung. Häufig werden sie mit der Beweissicherung bei Fällen konfrontiert, bei denen der Tatort nicht feststeht (*loss of location*). Franosch wies auf die noch andauernde Diskussion zu möglichen rechtlichen Lösungen für die Schwierigkeiten bei *loss of location* gespeicherter Daten im Internet hin. Beim *Cloud Computing* verlagert sich die Software mit großen Datenmengen zunehmend ins Internet. Clouds sind dabei dezentral organisiert und nicht auf einzelnen Servern zu lokalisieren. Selbst die Cloud-Computing-Provider dürften häufig nicht nachvollziehen können, wo bestimmte Daten zu einem bestimmten Zeitpunkt vorliegen. Das bedeutet, dass sich die Daten in verschiedenen Gerichtsbarkeiten/Rechtssystemen befinden. Dies verursacht große Probleme bei der Strafverfolgung. Computerdaten werden häufig außerhalb des nationalen Hoheitsgebiets gespeichert. Eine Recherche nach solchen Daten, die *transborder search*, muss als Verletzung der Territorialität betrachtet werden. Demnach dürften die Strafverfolgungsbehörden streng genommen keine Ermittlungen im Internet durchführen, sobald die Gefahr besteht, dass das nationale Hoheitsgebiet überschritten wird. Bei grenzüberschreitenden Strafverfolgungen werden die für die Ermittlungsverfahren relevanten Daten zunehmend auf ausländischen Servern gespeichert. Traditionelle Wege der internationalen Zusammenarbeit in diesen Strafsachen sind oft zu langsam, was zum Verlust von Beweisdaten führt. Rechtshilfeersuchen, ein traditionelles Instrument der transnationalen Zusammenarbeit, sind meist unwirksam bei Ermittlungen in Bezug auf das Internet. Dabei spielt der Zeitfaktor eine entscheidende Rolle, da in einigen Staaten keine Vorratsdatenspeicherung vorgenommen wird. Die Strafverfolgungsbehörden sind dennoch verpflichtet, die Kriminalität im Netz zu verfolgen. Im „Budapester Übereinkommen über Computerkriminalität"[3] von 2001 ist der grenzüberschreitende Übergriff auf Daten geregelt. Laut Franosch bietet das Übereinkommen keine ausreichenden Ermittlungsmöglichkeiten in dringenden Fällen. Insbesondere ist es dann unbefriedigend, wenn schnell auf im Ausland gespeicherte und nicht frei zugängliche Daten zugegriffen werden soll. Die Umsetzung einer internationalen vertraglichen Vereinbarung für den

---

[3] Übereinkommen über Computerkriminalität, Budapest, 23. 11. 2001 (bereinigte Übersetzung der zwischen Deutschland, Österreich und der Schweiz abgestimmten Fassung): http://conventions.coe.int/Treaty/GER/Treaties/Html/185.htm.

Zugang zu Daten, die auf Servern in Drittländern gespeichert sind, ist von entscheidender Bedeutung. Für die Bekämpfung der Cyberkriminalität und der Geldwäsche im Internet sind demnach neue internationale operative Partnerschaften, nicht nur bei der Polizei, sondern auch bei den Staatsanwaltschaften, erforderlich.

Supervisor Special Agent **Brian T. Herrick**, *Federal Bureau of Investigation*, informierte die Zuhörer in seinem Kurzvortrag **„Cybercrime Networking: Important to criminals, essential for policing"** über die Zuständigkeit des FBI im Bereich Cybercrime und seine Tätigkeit als US-Verbindungsbeamter in Deutschland.

Das FBI ist eine Sicherheitsbehörde mit Zuständigkeiten bei der Strafverfolgung und im nachrichtendienstlichen Bereich. Es ist u. a. zuständig für die Bekämpfung von Cyberkriminellen und hoch technisierten Angriffen. Das FBI hat im Ausland mehr als 60 Dienststellen, sogenannte "legal attachés", die in den US-Botschaften weltweit verortet sind. Um die Gefahr durch Cybercrime effektiv zu bekämpfen, seien Partnerschaften mit internationalen Strafverfolgungsbehörden notwendig. Der moderne Ermittler im Bereich Cybercrime müsse die Gesetze sowohl seines eigenen als auch der anderen Länder und die Ermittlungsmöglichkeiten verstehen und umsetzen können. Um dies effektiv durchzuführen, müssen personelle Kontakte und Partnerschaften aufgebaut werden. Das FBI arbeitet im Bereich Cybercrime eng mit der Industrie und internationalen Partnern zusammen. Beim FBI ist die zur Abwehr der Bedrohung eingerichtete *National Cyber Investigative Joint Task Force* (NCIJTF) angesiedelt, an der 19 Behörden aus den Bereichen Strafverfolgung und Nachrichtendienste beteiligt sind. In Deutschland werden regelmäßig über die festgestellte IP-Adresse bzw. den ISP Bezüge zu den USA festgestellt. Die US-amerikanischen Strafverfolgungsbehörden sind sehr aktiv im Bereich der Bekämpfung der Cybercrime und gehören zu den wichtigsten Kooperationspartnern Deutschlands.[4]

---

[4] Weitere Informationen: http://www.fbi.gov/about-us, http://www.fbi.gov/about-us/partnerships _and_outreach/.

Die Gesichter der OK:
7. Forschungskonferenz Organisierte Kriminalität in Wiesbaden, 2014

Vom 8. bis 9. Oktober 2014 fand im Bundeskriminalamt in Wiesbaden die 7. OK-Forschungskonferenz zum Thema „The different Faces of Organised Crime" statt. Ihr Themenschwerpunkt lag auf den Forschungsaktivitäten und der Darstellung der Lage zu den „Gesichtern" der OK. Sechs der acht Redner referierten über die OK in Deutschland, dem Vereinigten Königreich, den Niederlanden und in Schweden. In einem Vortrag aus Schweden wurde über eine neue Kriminalitätsform der OK, den „Sozialbetrug", berichtet. Dieser wird der OK zugeordnet, sofern er organisiert begangen wird. Aus Schweden wurde darüber hinaus der *Arboristic Approach* zur OK-Bekämpfung vorgestellt. Eine Vertreterin der *National Crime Agency* (NCA), London, berichtete über die britische OK-Bekämpfungsstrategie 2014/2015. Aus den Niederlanden wurde zur Herstellung synthetischer Drogen aus chemischen Vorläufersubstanzen und zur Umsetzung der Erkenntnisse aus der Analyse von OK-Verfahren bei der Strafverfolgung im Rahmen der OK-Bekämpfung vorgetragen. In der Präsentation aus Deutschland wurden die dort dominierenden Formen der OK beschrieben. In weiteren Vorträgen wurde die russische Mafia in Eurasien und Europa dargestellt und die „Global Initiative against Transnational Crime" präsentiert.

Der Leitende Kriminaldirektor beim Bundeskriminalamt **Stefan Michel** beschrieb in seinem Vortrag **„The different faces of organised crime"** die unterschiedlichen Facetten der schweren und Organisierten Kriminalität in Deutschland und gab einen Überblick über die neuesten Entwicklungen und Herausforderungen für die Polizei.

Die Zahl der in Deutschland geführten OK-Verfahren bewegt sich seit zehn Jahren in einem Korridor um 600 pro Jahr bei etwa ca. 9.000 Tatverdächtigen. Dabei liegt eine enge OK-Definition zugrunde, die nur die besonders qualifizierten Begehungsweisen umfasst. Rund 600 OK-Verfahren stehen jedes Jahr mindestens 1.500 bis 2.000 Verfahren im Vorfeld der OK und 9.000 Tatverdächtige der OK ca. 20.000 bis 30.000 verdächtige Schwer- und Schwerstkriminelle gegenüber. Michel gab einen Überblick über die Cyberkriminalität, traditionelle und neue Formen von OK-Gruppen und zu den nachfolgend beschriebenen Erscheinungsformen, die das „Gesicht" der OK in Deutschland prägen.

In Deutschland gibt es ca. 9.000 Mitglieder von **Rockergruppierungen**, die in ca. 650 Chaptern/Chartern organisiert sind. Das Phänomen „Rockerkriminalität" ist von erheblicher Bedeutung und beschäftigt die Strafverfolgungs-

behörden in hohem Maße, zumal komplexer geworden ist. *Outlaw Motorcycle Gangs* (OMCG) verzeichnen einen Zulauf an neuen Mitgliedern und Unterstützern. Im Fokus stehen nicht nur die etablierten traditionellen Rockergruppierungen. Zahlreiche Neugründungen von Supporterclubs, rockerähnlichen Gruppierungen und Streetgangs stellen im Hinblick auf Auseinandersetzungen untereinander und mit den Etablierten ein zusätzliches Konfliktpotenzial dar. OMCG sind international vernetzt und kooperieren teilweise mit anderen OK-Gruppierungen.

In Deutschland haben sich **russisch-eurasische OK-Strukturen** über die Jahre fest etabliert. Die russisch-eurasische OK versteht sich als Parallelgesellschaft mit eigenem Werte- und Normensystem. Die Ideologie der „Diebe im Gesetz" ist in Teilen in der russischsprachigen Gemeinschaft in Deutschland – etwa 4,5 Mio. Menschen – verwurzelt. Besonders deutlich ist die Verbreitung dieser Ideologie in den deutschen Justizvollzugsanstalten zu beobachten, in denen permanent etwa 4.500 bis 5.500 russischstämmige/-sprachige Häftlinge einsitzen. Im Fokus europäischer Ermittlungsbehörden stehen insbesondere russisch-eurasische Straftätergruppierungen, die überwiegend im Bereich der organisierten Eigentumskriminalität in Form von Ladendiebstahl und Einbruchsdiebstahl in Erscheinung treten.

Für die **italienische Mafia** ist Deutschland nach wie vor in erster Linie Ruheund Rückzugsraum. In den letzten 15 Jahren wurden insgesamt 244 OK-Verfahren gegen italienische OK-Gruppierungen geführt. Im Rahmen einer deutsch-italienischen Arbeitsgruppe wurde Mitte der 1990er Jahre ein Überblick über die Präsenz von Mafia-Angehörigen in Deutschland gewonnen. Dies führte u. a. dazu, dass 1995–2014 314 Mafia-Mitglieder wegen verschiedener Straftaten in Italien, darunter mehrere Mordtaten, in Deutschland festgenommen werden konnten. Daneben besteht seit dem sechsfachen Mord 2007 in Duisburg eine deutsch-italienische *Task Force*, die einen optimierten polizeilichen Informationsaustausch und intensivere operative Zusammenarbeit zum Ziel hat.

Weiterhin gibt es Kriminalitätserscheinungsformen, die als vermeintliche Massendelikte zumindest der banden- und gewerbsmäßigen Kriminalität zuzurechnen und in Teilbereichen auch in international agierende OK-Strukturen eingebettet sind. Hierzu zählt der **organisierte Betrug durch Callcenter.** Seit mehreren Jahren werden Betrugsstraftaten festgestellt, bei denen die Anbahnung durch Callcenter überwiegend in der Türkei erfolgt. Dabei werden von den Anrufern Gewinnversprechen gegen Vorleistungen gemacht bzw. Drohszenarien aufgebaut und unberechtigte Forderungen erhoben. Opfer sind überwiegend ältere Menschen, wobei das Hellfeld auf höchstens 10 % geschätzt wird. Die Täterstrukturen agieren organisiert und grenzüberschreitend und gehen arbeitsteilig vor. Die Kommunikation mittels VoIP wird meist ma-

nipuliert, um Anrufe aus der Türkei zu verschleiern und polizeiliche Ermittlungsmaßnahmen zu verhindern.

Ein weiteres Beispiel ist die **strukturelle Eigentumskriminalität im Bereich des Wohnungseinbruchsdiebstahls,** begangen durch reisende Tätergruppen**. In Deutschland sind die Fallzahlen des Wohnungseinbruchsdiebstahls bis 2006 zurückgegangen, steigen seitdem aber stetig an. Der Anstieg ist im Wesentlichen auf Täter bzw. Tätergruppierungen aus Südost- und Osteuropa zurückzuführen. Die Täter reisen aus dem Ausland zur Straftatenbegehung nach Deutschland ein und bleiben mitunter wochen- oder gar monatelang, um entweder ausschließlich Wohnungseinbruchsdiebstähle oder auch andere Straftaten zu begehen. Sie bedienen sich oft sogenannter „Residenten", in der Regel Landsleute, die sich um die Beschaffung von Fahrzeugen, Wohnungen und Papieren kümmern sowie im Festnahmefall Rechtsanwälte vermitteln. Die Residenten fungieren auch als Hinweisgeber für geeignete Einbruchsobjekte/-wohngegenden und kümmern sich um die Verwertung des Diebesguts.

Die Präsentation über die **„Mafia and Anti-Mafia in Eurasia: the Specificity of Post-Soviet Georgia"** von **Dr. Gavin Slade**, Kriminologe und Forschungsstipendiat an der Freien Universität Berlin und der Dahlem Research School, stützte sich auf die Untersuchung der Rolle und Wirkung der Organisierten Kriminalität in Georgien. Seine Ergebnisse basieren auf seinen Forschungsarbeiten der vergangenen sieben Jahre.

Slade stellte dar, dass die überwiegende Mehrzahl der Mitglieder der russischen Mafia aufgrund diverser Vorfälle wie der Operation Java im Jahre 2010 oder dem Mordfall „Japontschik" im Jahre 2009 verhaftet wurde. Es sei erstaunlich, dass Georgier nur 2 % der sowjetischen Bevölkerung ausmachten, aber ein Drittel der erfahrenen „Diebe im Gesetz" (*thieves in law*) stellen. Zum Hintergrund wurde erläutert, dass „Diebe im Gesetz" eine Hinterlassenschaft des Gulags sind und erstmals gegen Ende der 1920er auftauchten. Slade erläuterte, dass der Grund, weshalb georgische Straftäter so intensiv in der OK aktiv sind, mit dem Ende der Sowjetunion zusammenhängt, auf das in Georgien einen staatlicher Zusammenbruch folgte. Von allen früheren Sowjetrepubliken war nur der Kollaps des tadschikischen Staats noch folgenreicher. Angesichts dieser Entwicklungen bestand in Georgien eine starke Nachfrage nach Sicherheits- und Schutzdiensten. Darüber hinaus hatte Georgien einen der größten Schwarzmärkte in der Sowjetunion, Die Romantisierung von Dieben in der georgischen Gesellschaft, die sich auch in der Sozialisierung von Kindern wiederfindet, spiegelte sich in einer Umfrage aus dem Jahre 1993 wider, wonach 25 % der Schulkinder in Tiflis später „Dieb im Gesetz" werden wollten. Allerdings hat sich diese Situation durch die Rosenrevolution 2003 und eine sehr strenge Antimafia-Gesetzgebung sowie tief-

greifende Reformen drastisch verändert, denen die sizilianischen Kampagnen und Modelle als Vorbild dienten. Die Null-Toleranz-Politik veranschaulicht auch die von 6.119 im Jahre 2003 auf 23.864 im Jahre 2010 dramatisch angestiegene Zahl der Strafgefangenen und ein Zitat Micheil Saakaschwilis, georgischer Präsidenten von 2004 bis 2013, wonach die größten Exporte nach Russland nicht mehr Wein, sondern „Diebe im Gesetz" seien. 10 % der georgischen „Diebe im Gesetz" gehen nach Europa, Israel und in die GUS-Staaten. Überdies bemerkenswert ist, dass die meisten Diebe aus nur drei georgischen Regionen stammen, darunter auch aus Abchasien. Mitglieder der postsowjetischen OK-Gruppen sind gut miteinander vernetzt – wohl eine Hinterlassenschaft des Gulags – und verfügen über eine ausgeprägte Mobilität. Die Verlagerung der OK-Gruppen ins Ausland ist dennoch schwierig. Es wurde erläutert, dass die „Diebe im Gesetz" aus einer relativ homogenen straffälligen Subkultur stammen, in der sich Praktiken wie beispielsweise ein Ehrenkodex und Tätowierungen entwickelt haben, um mit den aufgrund der Lagerstruktur und der hohen Fluktuation und Bewegung der Strafgefangenen entstehenden Ungewissheit umzugehen. Traditionelle Mechanismen, die kollektives Handeln und Koordinierung ermöglichen, und die Tatsache, dass die Diebe auch über Volksgruppen hinweg arbeiten, haben die Ausbreitung der postsowjetischen OK ermöglicht.

In der Präsentation mit dem Titel **„The Global Initiative against Transnational Organized Crime – Exploring new Challenges and Responses"** befasste sich **Botschafter Dr. Ugljesa Zvekic** mit der Gründung der *Global Initiative against Transnational Organized Crime* und stellte deren Geschichte, Herausforderungen, Ziele und Kontext vor.

In den letzten Jahren haben sich Größe und Reichweite der Organisierten Kriminalität dramatisch verändert, d. h. nicht nur Verlagerungen großer illegaler Märkte stattgefunden. Insbesondere in „schwachen" Staaten stellt die OK eine enorme Bedrohung dar, weil kriminelle Aktivitäten kumuliert auftreten und sich Unsicherheit und Gewalt verbreiten, wenn Kontrolle über Personengruppen ausgeübt wird. Selbst in höher entwickelten Staaten hat die OK eine enorme Wirkung auf staatliche Stabilität, Regierungsführung und Entwicklung. Außerdem gibt es nur wenige internationale Abkommen im Bereich der Organisierten Kriminalität; am bedeutendsten ist das Palermo-Übereinkommen. Zvekic führte aus, dass das Palermo-Übereinkommen jedoch einseitig zugunsten der Strafverfolgungsbehörden formuliert, überholt, nicht wirksam und zu alt sei, sodass eine neue Plattform für strategisches Engagement erforderlich gewesen sei. Daraus resultierte die Gründung der *Global Initiative* – ein Netzwerk verschiedener Akteure, das sich aus Hintergrundgesprächen entwickelt hat. Zu ihren Zielen zählen strategische, analytische und reaktive Vorgehensweisen, um wirksamere Reaktionsmöglichkeiten gegen Organisier-

te Kriminalität zu entwickeln und ein Netzwerk mit Ressourcen für internationale Partnerschaften aufzubauen. Die Initiative gliedert sich in mehr als 100 Teilnehmer, einen Beirat und ein in Genf ansässiges Sekretariat, für das die Schweizer Regierung Räumlichkeiten zur Verfügung stellt. Insbesondere wird die Initiative nicht von der Regierung geleitet und zeichnet sich durch einen speziellen, die Flexibilität steigernden Ansatz aus, weil sie keine politischen Überlegungen und Argumente zu beachten hat. Zu den prioritären Bereichen der Initiative zählen Umweltstraftaten, Governance, fragile Staatlichkeit und Entwicklung sowie Cybercrime. Bisher fehlt eine Auswertung der Umsetzung des Palermo-Übereinkommens in Problemländern, da sie von mehreren Regierungen blockiert wird. Zvekic betonte, dass der direkte Zusammenhang der OK mit Armut, Bildung, Zugang zu Mikrokrediten etc. zu beachten ist. Ein ganzheitlicher Ansatz nicht nur aus Perspektive der Regierungen und Strafverfolgungsbehörden ist notwendig, denn die OK muss in Verbindung mit Entwicklungsfragen angegangen und analysiert werden. Ganz im Gegenteil sind OK-Theorien aber von Entwicklungstheorien abgekoppelt.

Wissenschaftliche Forschung und Polizeipraxis waren das Thema der Präsentation von **Prof. Dr Edward Kleemans** von der Fakultät für Rechtswissenschaften der Freien Universität Amsterdam. In seinem Vortrag mit dem Titel **„Organised crime as transit crime and what it means for criminal investigation" (OK als Transitkriminalität und die Konsequenzen für Ermittlungsverfahren)** sprach Kleemans unter anderem über die OK-Struktur in den Niederlanden, den niederländischen *Organised Crime Monitor* (OK-Monitor) und darüber, dass die Einblicke in OK-Strukturen eine Änderung von Ermittlungsstrategien, internationaler Kooperation und Prävention ausgelöst haben.

Kleemans beschrieb, dass im Gegensatz zu italienischen Mafiagruppen die OK-Gruppen in den Niederlanden nicht hierarchisch, sondern eher netzwerkartig aufgebaut sind. OK-Gruppen machen ihre größten Gewinne nicht lokal, sondern mit Schleusung und Menschenhandel. Daher haben ihre Vergehen einen internationalen Kontext. In den Niederlanden ist Transitkriminalität vorherrschend, die sich auf Handel und Grenzüberschreitung konzentriert. Studien zu Transitstraftaten konnten herausarbeiten, dass viele normale Unternehmen wie Speditionen, Reisebüros etc. in die Logistik der Transitkriminalität eingebunden sind. Ihre Profitabilität ist wesentlich dafür verantwortlich, dass „Transitstraftaten" bei vielen OK-Gruppen die Hauptaktivität ausmachen. Dies gilt für die Drogenproduktion und den Import und Export. Attraktive Gewinne lassen sich auch durch Schleusung illegaler Einwanderer und hochbesteuerter Waren erzielen. Um einen besseren Einblick in das Wesen Organisierter Kriminalität zu erhalten und die Polizeipolitik und -praxis

zu verbessern, erhielt das *Dutch Research and Documentation Centre* den Auftrag, das laufende Forschungsprojekt mit dem Titel „Dutch Organised Crime Monitor" durchzuführen. Im Rahmen dieses Monitors wird alle vier Jahre ein auf die Analyse 40 umfangreicher polizeilicher Ermittlungen über kriminelle Gruppen in den Niederlanden gestützter Bericht veröffentlicht. Informationen stammen auch aus öffentlich verfügbaren und vertraulichen Berichten, Kriminalitätsanalysen und Interviews mit Experten vor Ort. Zwischen 1996 und 2012 wurden 150 umfangreiche Ermittlungsverfahren systematisch analysiert, sodass Folgendes abgeleitet werden konnte:

– Konsequenzen für Ermittlungsstrategien

Heute konzentrieren sich die niederländischen Strafverfolgungsbehörden vorrangig auf wichtige Personen einer Gruppe (Vermittler) und nicht mehr ausschließlich auf deren Bosse/Führer. Vermittler sind häufig wichtiger als der Boss, weil sie die Gruppe in Betrieb halten.

– Konsequenzen für die internationale Kooperation

Mehr internationale Kooperation bedeutet einen dauernden Wissens- und Informationsaustausch, wobei die Prioritäten der Partnerländer und die Übertragung von Zuständigkeiten von der lokalen auf die nationale Ebene berücksichtigt werden.

– Konsequenzen für die Prävention

Laut Forschung bestehen bestimmte Kriminalitätschancen. Daher wurde das *Barrier Model* entwickelt, das Menschenhandel als geschäftliche Unternehmung betrachtet, die eine Reihe von Hindernissen überwinden muss, bevor Menschenhändler durch Ausbeutung anderer Geld zu verdienen beginnen. Ziel ist es, für die Menschenhändler die Barrieren zu erhöhen, sodass Menschenhandel schwieriger, weniger lukrativ und damit weniger attraktiv wird. Derartige Barrieren sind Rekrutierung, Zutritt, Identität, psychologische Bindung, Unterbringung, Arbeit und finanzielle Aspekte.

Eine große Veränderung der vergangenen zehn Jahre ist der zunehmende Einsatz flexibler, schneller Einsatzstrategien als Alternative zu früheren umfassenden und langfristigen polizeilichen Ermittlungen. Verhaftungen und Zugriffe in OK-Netzen wurden nicht mehr um jeden Preis zurückgestellt oder verhindert, sondern mitunter absichtlich eingesetzt, um Beweise gegen die Hauptverdächtigen zu sammeln. Schnelle Interventionen werden jetzt häufig mit langfristigen Ermittlungsstrategien gekoppelt. Dies geht auch mit einem stärkeren Fokus auf Vermittler in kriminellen Netzwerken und die Rolle eines fördernden Umfelds einher. Der sogenannte administrative Ansatz, bei dem

lokale Regierungen und andere Partner in die OK-Bekämpfung und -Prävention eingebunden sind, wird in den Niederlanden sehr positiv aufgenommen.[1]

Matthijs Vijlbrief von der *Central Intelligence Division* der nationalen niederländischen Polizei beschrieb in seinem Vortrag **„Trends and developements in Dutch organised synthetic drugs crime: a cat and mouse game"** die Herstellung synthetischer Drogen, insbesondere Amphetaminen, in den Niederlanden.

Vijlbrief sieht die Niederlande als globales Hauptproduktionsland für synthetische Drogen. 2013 wurden 57 Drogenlabore und 120 Lagerplätze für Amphetamine und MDMA (3,4-Methylendioxy-N-methylamphetamin) sichergestellt. Die geschätzte jährliche Produktion für Amphetamine betrug 80 000 Kilo und für MDMA 150 Millionen Tabletten. Im illegalen Großhandel werden jährlich 200 Millionen Euro umgesetzt. Dies bedeutet einen Straßenhandelspreis von zwei Milliarden Euro. Wesentliche Chemikalien für die Produktion synthetischer Drogen sind PMK (Piperonylmethylketon), BMK (Benzylmethylketon), GBL (Gamma-Butyrolacton), Ephedrin und Lysergsäure. PMK wird in Asien aus safrolhaltigen Ölen aus Baumwurzeln gewonnen und legal sehr begrenzt für die Herstellung von Parfüm genutzt. Seit der Wiener Konvention von 1988 wird die Herstellung international kontrolliert. PMK wird von China nach Westeuropa, insbesondere in die Niederlande transportiert und zur illegalen Herstellung von MDMA genutzt. Aus einem Liter PMK lässt sich ein Kilo MDMA herstellen, womit ca. 10 000 XTC-Tabletten produziert werden können.

Auch BMK, das in der Vergangenheit aus China bezogen wurde, wird sowohl legal als auch illegal in chemischen Fabriken in den Niederlanden produziert und zur Herstellung von Amphetaminen verwendet. Legal wird die Substanz z. B. für die Herstellung von Rattengift verwendet. Seit der Wiener Konvention von 1988 wird die Produktion international kontrolliert. Vor-Vorläufersubstanzen sind Chemikalien, die zur Herstellung von Vorläufersubstanzen illegaler Betäubungsmittel dienen. Meist ist für die Herstellung nur ein zusätzlicher, oft sogar legaler Prozess notwendig. In den Niederlanden wird eine ganze Reihe von Vor-Vorläufersubstanzen produziert. So wurden bei einer polizeilichen Durchsuchung im Jahr 2010 zwei Tonnen des Stoffs APAAN (Alpha-Phenylaceton-Acetonitril), ein für Haut, Augen und Atem-

---

[1] Weitere Informationen zu „Applied Police Research – Challenges and Opportunities" (Angewandte Polizeiforschung – Herausforderungen und Chancen), herausgegeben von Ella Cockbain und Johannes Knutsson, Crime Science Series, Book Routledge, zuerst erschienen 2015; Beitrag von E. R. Kleemans: „Police data and academic research" (Polizeidaten und akademische Forschung): https://books.google.de/books?id=kaDBAAAQBAJ&pg=PA64&dq=Kleemans+investigation+strategies&hl=en&sa=X&ved=0CCAQ6AEwAGoVChMIlrXrwtfhxgIVw rgUCh0ZkwTy#v=onepage&q=Kleemans%20investigation%20strategies&f=false.

wege extrem gesundheitsgefährliches weiß-graues Pulver, sichergestellt. Aufgrund der Eignung als Ausgangsstoff für die Metamphetaminsynthese gehören Phenylaceton in der EU und der Schweiz nach dem Grundstoffüberwachungsgesetz zu den verbotenen Stoffen. Im Februar 2011 wurde das erste Labor für die Umwandlung von APAAN in BMK beschlagnahmt. Die Niederlande werden seit 2011 mit in China produziertem APAAN, für das keine legale Nutzung bestimmt ist, überschwemmt. Bis Ende 2013 gab es für die Substanz in der gesamten EU keine Produktions- und Handelsbeschränkungen. In den Niederlanden geht man davon aus, dass 2012 50 % aller sichergestellten Amphetamine (Speed) mit APAAN hergestellt wurden; 2013 bereits über 75 %. Grund für die wachsende Bedeutung der Substanz ist die Tatsache, dass im Rahmen eines einfachen chemischen Prozesses die Vorläufersubstanz BMK gewonnen werden kann. Es gibt dafür drei verschiedene Konversionsmethoden: 1. mit Sulphuric Acid (Schwefelsäure), dabei können etwa 60 % des Stoffes verwertet werden. 2. mit Phosphoric Acid (Phosphorsäure) sind dies bereits 70 %. 3. mit Hydrochloric Acid (Salzsäure) können 80 % zur Herstellung von BMK verwertet werden. Die höchste Qualität wird mit Sulphuric Acid erzielt. Die Verwendung von Hydrochloric Acid ist am effektivsten, aber auch für die Gesundheit am gefährlichsten. Für Drogenproduzenten bedeutet die Verwendung von APAAN einen höheren Profit: Zur Produktion einen Liters BMK waren bisher 800 Euro notwendig, jetzt sind es nur noch 60 Euro. Der Großhandelspreis für ein Kilo Amphetamin ist jedoch gleich geblieben. Dies führte zu einer Zunahme der Verfügbarkeit von BMK. Die Anzahl der Produktionsstätten stieg von 36 im Jahr 2011 auf 66 Ende des Jahres 2014 und die Anzahl der Lagerstätten von 61 im Jahr 2011 auf 228 Ende 2014. Bei der Sicherstellung von APAAN-Laboren ist die Anwendung der üblichen Schutzmaßnahmen nicht ausreichend. Das Tragen chemischer Schutzanzüge und die zusätzliche Anwendung einer speziellen APAAN-Dekontamination-Prozedur sind erforderlich.

Laut Vijlbrief verhält es sich bei der illegalen Produktion synthetischer Drogen und deren Vorläufersubstanzen wie bei einem Katz- und Mausspiel. Als Reaktion auf die polizeilichen Maßnahmen sind eine ständige räumliche Verlagerung der Produktionsstätten und Lagerhallen und die Verwendung anderer chemischer Substanzen zu beobachten.

Kim Nilvall, Detective Inspector beim *Swedish National Bureau of Investigation* in Stockholm, hielt eine Präsentation mit dem Titel **„The Criminal Arboristic Approach – A method to combat organised crime"** über eine analytische Methode zur Identifizierung relevanter Personen der OK. Im Vortrag wurden der theoretische Hintergrund, die analytische Methodik, Ergebnisse und der Mehrwert im Zusammenhang mit dem *Criminal Arboristic Approach* skizziert.

Organisierte Kriminalität wird häufig mittels Begriffen wie ‚Banden‘, ‚Konstellationen‘, ‚Organisationen‘, ‚Clans‘, ‚OK-Gruppen‘, ‚Kartellen‘ etc. beschrieben und definiert. Daher ist ein entsprechender Ansatz notwendig, um OK anzugehen und einzuschätzen. Nilvall verwies auf die allgemeine Tatsache, dass Individuen Netzwerke kontaktieren. Straftäter kontaktieren kriminelle Netzwerke und lernen dort neue Personen kennen. Von entscheidender Bedeutung ist zu verstehen, warum manche Personen gemeinsam Straftaten begehen. Als Beispiel wurde der Facebook-Account eines Straftäters (Verkäufer von Cannabis) angeführt, dessen verschiedene Freundesgruppen analysiert wurden. Man entdeckte fünf Freundes-Cluster, zu denen neue untergeordnete Cluster hinzukamen. Bereits polizeibekannte Personen wurden identifiziert. Dadurch konnte man sich auf das Cluster der kriminellen Freunde konzentrieren. Die Zusammensetzung eines persönlichen Kontaktnetzwerks wurde angesprochen. Soziale Umstände verändern das Netzwerk jedes Individuums, die daher eher veränderlich als statisch sind. Abhängig vom Vertrauen besteht auch ein äußerer Kontaktkreis, in dem an die Aktivitäten angepasst andere Kontaktpersonen gesucht werden. Dabei wird eine Risikominimierung angestrebt, d. h. vermeintlich nicht vertrauenswürdige Personen gehören zum äußeren Kreis. Dieses Verhalten kann man als gewisse Form der Risikobewertung verstehen. Nilvall analysierte den Umfang krimineller Netzwerke und entwickelte einen Erklärungsansatz mit sechs Separationsgraden. Weil Schweden kein großes Land ist, seien alle dortigen Straftäter über wenige Separationsgrade verbunden. OK in Schweden kann demnach als Struktur mehrerer individueller krimineller Kontaktnetze, die Teil eines großen kriminellen Netzwerks sind, begriffen werden. Anhand der *Criminal Arboristic Perspective* (CAP) lassen sich die Auswirkungen von Kriminalität prognostizieren. Wichtige Personen in einem kriminellen Netzwerk sind diejenigen, die es am Leben halten, die Finanzen managen und neue kriminelle Aktivitäten entwickeln können. Nilvall erläuterte, wie man das Kontaktnetzwerk einer Person – Umfang, Grad der Nähe und des Vertrauens einer Beziehung, Kapazitätsbewertung und Priorisierung strategischer Personen – abbildet und den inneren Kontaktzirkel definiert.

Nilvall präsentierte zudem das *Personal Analysis Document* (PAD), das alle relevanten Informationen zu einem Straftäter enthält und damit einen taktischen Bericht über das Individuum liefert. Jede der 21 Polizeibehörden in Schweden erhält das PAD jedes Straftäters von strategischer Bedeutung, was die operative Transparenz erhöht. Norwegen und Schweden verwenden bereits dieselbe PAD-Methode und Nilvall betonte, damit auf einen europäischen Ansatz abzuzielen, um Straftäter mit strategischer Bedeutung in ganz Europa identifizieren zu können.

Thomas Falk, der Leiter der *Swedish Social Insurance Agency's Special Unit against Serious Organised Crime* (Sondereinheit gegen OK bei der schwe-

dischen Sozialversicherungsbehörde) in Hägersten, hielt eine Präsentation zum Thema **„The new Swedish model – combating benefit fraud in a welfare state" (Bekämpfung von Leistungsbetrug in einem Wohlfahrtsstaat)**.

Organisierter Leistungsbetrug ist in Schweden ein großes Problem. Das schwedische Wohlfahrtssystem finanziert sich über die Einkommensteuer und bietet diverse Missbrauchsmöglichkeiten. 2009 begannen mehrere schwedische Behörden eine Kooperation zur Bekämpfung von Leistungsbetrug. Bis zu diesem Zeitpunkt war nicht sicher, ob es sich bei Leistungsbetrug um ein lokales oder ein nationales Problem handelt. Anfang 2011 startete die schwedische Sozialversicherungsagentur das *Assistance Project*, eine nationale Monitoring-Kampagne, um falsche Unterstützungsbeihilfezahlungen zu entdecken und zu verhindern. Das Projekt wird im Rahmen des *Regional Intelligence Center* (RUC) in Kooperation mit Polizei, Staatsanwaltschaft, schwedischer Steuerbehörde und anderen Behörden durchgeführt. 2013 arbeiteten ca. 40 speziell ausgebildete Ermittler an Kontrollermittlungen zur Unterstützungsbeihilfe. Eine der Ermittlungen lief gegen ein Pflegeunternehmen in Södertälje, das wegen einer Serie von Unregelmäßigkeiten bekannt war. Das Unternehmen war für die Pflege von 36 Klienten zuständig und beschäftigte etwa 240 Assistenten. Es wurden Verbindungen zum sogenannten Södertälje-Netzwerk festgestellt und der Fall wurde Teil des Projekts „Tore 2", einer gemeinsamen, behördenübergreifenden und von der Polizei operativ unterstützten Initiative gegen das kriminelle Netzwerk in Södertälje. In Södertälje bei Stockholm hat sich demnach eine von Falk so bezeichnete Parallelgesellschaft unter Teilen der dortigen syrischen Bevölkerung entwickelt. Zu ihr gehören die meisten Restaurants, Cafés und andere Branchen mit Bargeldverkehr in der Stadt. Die Parallelgesellschaft betreibt ihre eigene Schattenwirtschaft, ihr eigenes Strafrecht, Bank- und Kreditwesen und führt kriminelle Aktivitäten wie Drogenschmuggel und Erpressung durch. Teil dieses kriminellen Netzwerks sind Manager im Stadtrat von Södertälje und ein Parlamentsmitglied. Bisher wurden 533 Fälle von Entschädigungsbetrug (*compensation fraud*) untersucht.

In Schweden gibt es viele Herausforderungen im Zusammenhang mit Betrug gegen das Sozialversicherungssystem, zum Beispiel bei der zahnärztlichen Versicherung und am Arbeitsmarkt. Straftäter begehen Identitätsbetrug und kaufen Unternehmen, die als Fassade für ihre illegalen Tätigkeiten und kriminellen Aktivitäten genutzt werden.

„The different Faces of organised Crime in the UK" waren das Thema der Präsentation von **Sarah Groenewegen**, Senior Strategic Intelligence Analyst des *Picture of the Threat Team* bei der *National Crime Agency* NCA) in London. In ihrem Vortrag gab sie einen Überblick über das *British National Stra-*

tegic Assessment 2014/2015, eine Strategie zur Bekämpfung schwerer und Organisierter Kriminalität im Vereinigten Königreich.

Die *National Strategic Assessment* 2014 basiert auf Analyseberichten aus dem gesamten Vereinigten Königreich und liefert einen nationalen Überblick für alle Stakeholder, einschließlich Polizei und Regierung. Ziel ist es, zielgerichtet gegen schwere und organisierte Straftäter vorzugehen. Im Vereinigten Königreich gibt es keine offizielle OK-Definition, mit der man flexibler und anpassungsfähiger handeln könnte. Generell finden schwere und Organisierte Kriminalität dort in lockeren Netzwerken statt. Einzelpersonen, Paare oder Kleingruppen kontaktieren weitere Personen, um in verschiedenen Phänomenbereichen bei kriminellen Vorhaben zusammenzuarbeiten. Ein Teil der Straftaten schwerer und Organisierter Kriminalität wird von hierarchisch aufgebauten Gruppen aus engeren Kontaktpersonen und/oder Familienmitgliedern begangen, die teilweise im Ausland ansässig sind. Durch die sogenannte „Kartierung Organisierter Gruppen" werden 40 bis 50 Gruppen mit hoher Priorität eingestuft. Groenewegen erläuterte, dass OK im Vereinigten Königreich auch regionsspezifisch ist. In London sind beispielsweise überwiegend multiethnische Gruppen tätig. Der größte Teil der OK-Kriminellen sind Drogenschmuggler. Organisierte Gruppen im Bereich des Rauschgiftschmuggels sind häufig auch an der sog. Akquisitionskriminalität, wie gewerbsmäßiger Raub, organisierte Kfz-Verschiebung, organisierter Einbruchsdiebstahl (vorzugsweise von Metallen, Juwelen, Smartphones) und illegaler Handel geschützter Tierarten, beteiligt. Zum illegalen Waffenhandel wurde angemerkt, dass die meisten Taten mit Schusswaffengebrauch von Mitgliedern städtischer Straßengangs begangen werden. Groenewegen erläuterte, dass es sich bei organisierter Schleusungskriminalität und Menschenhandel einschließlich moderner Sklaverei um weitere relevante kriminelle Phänomene handele. Beim Menschenschmuggel profitieren Kriminelle in erster Linie von der Migrationsbewegung. Illegale Migranten werden häufig durch Menschenhandel ausgebeutet. Moderne Sklaverei unterteilt sich in die Kategorien Zwangsarbeit und Knechtschaft. Der Kampf gegen sexuelle Ausbeutung und Kindesmissbrauch ist dabei priorisiert, weil in den vergangenen Jahren viele Fälle öffentlich bekannt wurden. Die Täter sind vorrangig Einzeltäter, aber auch in Gruppen tätig. Wirtschaftskriminalität und Cybercrime sind weitere prägende Aspekte der OK. Organisierte Straftäter nutzen Cyber-Tools „als Service" und den Schutzraum des Dark Web. Ein weiteres großes Problem sind die organisierten Straftäter in den Justizvollzugsanstalten und die unter *lifetime management* (lebenslanger Überwachung) Stehenden. Einige Hochrisikotäter begehen weiter Straftaten und koordinieren Straftaten aus dem Gefängnis. Die Mehrzahl koordiniert Rauschgiftschmuggel, einige wenige koordinieren Waffenlieferungen. OK-Straftäter sind ausgesprochen geschult, um kriminelle Möglichkeiten zu erkennen und auszunutzen. Die Polizei arbeitet daher eng mit dem Justizvollzug zusammen.

Die Bekämpfung internationaler OK-Gruppen: 8. Forschungskonferenz Organisierte Kriminalität in Mainz, 2015

Am 7. und 8. Oktober fand im InterCityHotel in Mainz zum achten Mal in Folge die OK-Forschungskonferenz statt, im Rahmen derer internationale OK-Gruppen hinsichtlich ihrer Struktur und ihres Bedrohungspotenzials beleuchtet wurden. Konferenzschwerpunkt waren Forschungsaktivitäten, OK-Lage, Bekämpfungsstrategien und Schwierigkeiten bei der Strafverfolgung. Themen waren u. a. russischsprachige OK-Gruppierungen in den USA, in Europa und Deutschland sowie deren Aktivitäten im Bereich Cybercrime, reisende Tätergruppierungen, Rockergruppen und osteuropäische Cybergruppen. Weitere Themen waren die Rolle von Eurojust bei der Kriminalitätsbekämpfung und die lokale Dimension bei der Bekämpfung des Menschenhandels. Praktiker und Wissenschaftler aus den USA, dem Vereinigten Königreich, den Niederlanden, Schweden, der Schweiz und aus Deutschland präsentierten ihre Sichtweisen.

Nach der Eröffnung durch die Direktorin des Kriminalistischen Instituts beim Bundeskriminalamt **Martina Link** gab **Ursula Töttel** einen Überblick über das Projekt und die jährlichen Forschungskonferenzen (siehe Teil I „EU-Projekt ‚Research Network on Organised Crime' 2010–2016").

Verflechtungen der Organisierten Kriminalität im Zusammenhang mit dem Entstehen von Oligarchen-Vermögen in Russland sowie die Beteiligung der russischen OK im virtuellen illegalen Handel und deren Ausmaß bezogen auf die internationale Geldwäsche in den weltweiten Banksystemen waren die Themen der Präsentation **„The Globalization of Russian-speaking organised Crime"** von **Dr. Louise Shelley**, Inhaberin des Hirst-Stiftungslehrstuhls, Universitätsprofessorin sowie Gründerin und Direktorin des *Terrorism, Transnational Crime and Corruption Center* (TraCCC) an der George Mason University.

Shelley befasst sich mit neuen, in der postsowjetischen Periode entstandenen netzwerkbasierten OK-Gruppen, die nicht wie Mafiaorganisationen hierarchisch aufgebaut sind, sondern angesichts ähnlicher wirtschaftlicher Interesse zusammenarbeiten. Außerdem bestehen sie aus einer Vielzahl von Akteuren von hochrangigen Regierungsbeamten bis zu korrupten Vermittlern, die mit flexiblen Netzwerkstrukturen arbeiten. Shelley erklärte, dass es für die Globalisierung der russischen OK drei Gründe gebe: erstens die Mobilität der Personen, zweitens die Geldbewegungen durch den postsowjetischen Raum und letztlich die führende Rolle russischsprachiger Straftäter bei der Entwicklung von Malware-, Spam-, Phishing-Programmen etc. Mit einem Verweis auf die Verbindung zwischen der Herkunft von Oligarchen-Vermögen und der Orga-

nisierten Kriminalität kritisierte Shelley, dass diese Verbindung in der Literatur generell ignoriert werde. Insbesondere im Vereinigten Königreich wird nach Erkenntnissen der Strafverfolgung die Beteiligung der OK beim Aufbau von Oligarchen-Vermögen deutlich: So wurden 47 Personen in der Aluminiumindustrie ermordet. OK-Netzwerke arbeiten mit Untergruppen außerhalb der postsowjetischen Länder, um ihre weiteren Vorhaben zu planen und ihr Vermögen anzulegen. Diese Straftäter sind mit großer Wahrscheinlichkeit von Ländern mit Visafreiheit oder bei der Einreise erteilten Visa aus tätig, weil dies für Straftäter der leichteste Weg ist, um in ein Land einzureisen. Außerdem gibt ihnen der Besitz von Auslandsvermögen die Möglichkeit, operative Basen in dem betreffenden Land einzurichten. OK-Vermittler sind „keine Schlägertruppe der Organisierten Kriminalität". Korruptionsvorgänge behindern die Überwachung in das Land einreisender Personen. Geldbewegungen werden durch den postsowjetischen Raum mithilfe von Tarnfirmen und Offshore-Konten abgewickelt. Shelley berichtete, dass viele Banken die Finanzströme auf den Konten ihrer Kunden nicht mit ausreichender Sorgfalt prüfen, was diese zu OK-Komplizen mache. Sie wies darauf hin, dass es sich bei den operativen OK-Zentren um die „üblichen Verdächtigen" wie Zypern, Dubai und Moldawien, aber auch Finanzzentren wie Liechtenstein handele. Daraus leitete Shelley Probleme bei der Bekämpfung ab: Manche Volkswirtschaften in EU-Mitgliedstaaten seinen vom Geld aus kriminellen Aktivitäten abhängig geworden. Die Mittel zur Verschleierung der Geldherkunft seien ungeheuer komplex und personalintensiv. Am Ende ihres Vortrags erläuterte Shelley, dass umfangreiche Netzwerkanalysen erforderlich seien sowie ein großer Bedarf an Personen bestehe, die die russische Sprache und Kultur verstehen.

Einen Beitrag zu grenzüberschreitenden Ermittlungen, der Arbeit auf unterschiedlichen Ebenen und den internationalen Koordinierungskonferenzen leistete Oberstaatsanwalt **Benedikt Welfens**, Stellvertretendes Nationales Mitglied für Deutschland und Vorsitzender des *Team Trafficking and Related Crimes* aus Den Haag, mit seiner Präsentation **„The Role of Eurojust in combating Organised Crime"**, in der er auch einen Überblick über die Wurzeln und die Entwicklung von Eurojust gab.

In der EU besteht eine enorme Vielfalt von Rechtssystemen, die natürlich die Bekämpfung internationaler Kriminalität beeinflusst. Aus der Notwendigkeit, daher über Wege zur Erleichterung internationaler Zusammenarbeit nachzudenken, entstand schließlich das Eurojust-Konzept. So erklärte Welfens, dass die Justiz insbesondere beim zwischen den EU-Mitgliedstaaten geschlossenen Rechtshilfe-Übereinkommen (MLA) normalerweise langsam handele. Außerdem steht die fehlende Kooperation bei grenzüberschreitenden Ermittlungen in der Kritik. Welfens hob dann den Eurojust-Beitrag auf internationaler Ebene hervor und beschrieb die praktischen Vorgehensweisen. Er

erwähnte konkrete Fälle, um die Funktion von Eurojust innerhalb der EU zu erläutern. So arbeitet Eurojust auf drei Ebenen: erstens in einer Plenarsitzung, zweitens unter Beteiligung ausschließlich nationaler Referate und drittens unter Teilnahme mit konkreten Fällen befasster Ermittler/Staatsanwälte/Richter. Diverse Drittländer, Kooperationspartner und internationale Organisationen wie Europol, der größte Teilnehmer an solchen Sitzungen, sind an den Koordinierungskonferenzen beteiligt. Prioritäre Kriminalitätsbereiche wie Betrug, Drogenschmuggel, (mobile) OK, Straftaten gegen die finanziellen Interessen der Union (PIF-Straftaten)[1] etc. machen 65 % der Arbeit aus, während 35 % als nicht prioritäre Kriminalitätsbereiche eingestuft werden. Ein weiterer bedeutsamer Wert von Eurojust liegt in der Finanzierung von *Joint Investigation Teams* (Gemeinsame Ermittlungsteams, JIT)[2], weil finanzielle oder organisatorische Zwänge im Zusammenhang mit der internationalen Struktur von Straftaten der überwiegend notwendigen Beteiligung nicht entgegenstehen sollten. Außerdem versetzt die Partizipation an der Finanzierung dieser Teams Europol in die Lage, Informationen zu konkreten Fällen zu sammeln und die Effektivität der JIT zu beurteilen. Als weitere Aufgabe von Eurojust betrachtet man die Intensivierung von Kooperationen und den Austausch mit Europol und Drittländern über Koordinierungssitzungen und -zentren. Außerdem präsentierte Welfens ein Fallbeispiel für Menschenhandel von Minderjährigen zur Begehung von Diebstählen: Ein bosnisches kriminelles Netzwerk schleuste minderjährige bosnische Mädchen ein, die vorwiegend im Pariser öffentlichen Nahverkehr Diebstähle verübten. Die Pariser Staatsanwaltschaft beantragte die Unterstützung von Eurojust bei der Koordinierung der in Frankreich und Bosnien-Herzegowina laufenden Ermittlungen. Zwei Koordinierungssitzungen wurden organisiert, bei denen sich die beteiligten Behörden in Den Haag bzw. Sarajevo trafen. Die französisch-bosnische Kooperation beinhaltete gemeinsame Ermittlungen, Observationen, das Abhören von Telefongesprächen sowie Durchsuchungen, Beschlagnahmen und Durchsetzungen von Haftbefehlen. Die Justizbehörden, die Polizei, NGOs und für den gesetzlichen Schutz Minderjähriger in Frankreich und Bosnien-Herzegowina zuständige Institutionen arbeiteten eng mit Eurojust zusammen, um diese Operation zum Erfolg zu führen.

So kann die Beteiligung von Eurojust an einem konkreten Fall – beispielsweise durch die Finanzierung gemeinsamer Teams, Rechtshilfe- und JIT-Beschleunigung, den Kontaktaufbau zwischen Netzwerken, die Lieferung nütz-

---

[1] Aus dem Französischen: „protection des intérêts financiers".

[2] Gemäß Europol-Definition: „Ein gemeinsames Ermittlungsteam (JIT) ist ein für einen definierten Zeitraum aufgrund einer Vereinbarung zwischen zwei oder mehr EU-Mitgliedstaaten und/oder zuständigen Behörden für einen bestimmten Zweck gebildetes Ermittlungsteam. EU-Drittländer können sich mit Zustimmung aller anderen Parteien an einem JIT beteiligen."

licher Informationen, Koordinierung der Maßnahmen von Justizbehörden im Zusammenhang mit Durchsuchungen, Festnahmen und Beschlagnahmen und nicht zuletzt durch die Vermeidung von Missverständnissen bei unterschiedlichen Rechtssystemen – die Ermittlungen unterstützen.

Der zweite Tag der Forschungskonferenz begann mit einer Präsentation von **Johan Lundberg**, Superintendent der Polizeidirektion Göteborg, Schweden. In seiner Präsentation mit dem Titel **„Mobile Eastern European Groups in Sweden – Project Metal Thefts"** skizzierte er die beiden Polizeioperationen „Kopparorm" und „CIRCA" sowie deren Planung, Durchführung und Ergebnisse.

Die „Operation Kopparorm" befasste sich mit Metalldiebstählen. Erste Ermittlungen wurden im Polizeibezirk Örebro eingeleitet, nachdem im Jahr 2004 Metalldiebstähle durch die lokalen Behörden als zunehmende Bedrohung festgestellt worden waren. Die Polizeidirektion Västra Götaland verfasste einen Bericht, der 2006 die Grundlage für die „Operation Kopparorm" bildete. Die Ermittlungen unter Führung der Polizeidirektion Västra Götaland ergaben, dass Metalldiebstähle sowohl eine Gefahr für die Öffentlichkeit als auch ein Risiko für die Infrastruktur darstellten. Die Analyse zeigte, dass Unternehmen in Göteborg gestohlene Metalle aus Diebstählen im ganzen Land angekauft hatten. Weil keine Belege existierten oder Bargeldzahlungen geleistet worden waren, war die Identifizierung der Verkäufer meist nicht möglich, sodass mit anderen Behörden wie beispielsweise der Steuerbehörde, der Behörde für Umweltstraftaten und Versicherungsunternehmen zusammengearbeitet werden musste. Außerdem umfassten die Vorschläge auch Maßnahmen zur Prävention von Straftaten wie beispielsweise wirksame Schließsysteme und Gesetzesänderungen. Zu den konkret zu ergreifenden Maßnahmen zählten: Überwachung des Umfelds, Gespräche mit Industrievertretern sowie Steuerprüfungen. Dies führte 2011 zur Verurteilung von fünf Personen, die einer größeren Gruppe von Metalldieben angehörten. Die Anführer dieser Tätergruppe stammten aus dem früheren Jugoslawien, die „Ausführenden" waren rumänischer Herkunft. Alle wurden zu Gefängnisstrafen von 25 Jahren verurteilt – durch Steuerstraftaten und Taten der Organisierten Kriminalität hatten sie Geld im Wert von 2,5 Millionen € gestohlen. Nach Aussage von Lundberg waren die Schlüsselfaktoren für diesen Erfolg die Bildung einer Bekämpfungseinheit mit nationaler Zuständigkeit, Kooperationen mit anderen Behörden wie beispielsweise denen in München, London, Finnland, Norwegen und Dänemark, aber auch die Beschaffung der notwendigen Ermittlungsressourcen und die Bereitstellung von Intelligence-Personal mit speziellem Fokus bei Europol, um die Nachhaltigkeit der Bekämpfung von Metalldiebstählen zu sichern.

Die „CIRCA"-Einheit wurde 2009 eingerichtet, hat ihre Wurzeln in Göteborg und Vårgårda und konzentriert sich auf eine spezielle ermittlungstechnische und internationale Perspektive. Straftäter werden als Beteiligte an „Mobilen OK-Gruppen" (*Mobile Organised Crime Groups*, MOCG) identifiziert, die häufig aus Bulgarien und Rumänien stammen und für diverse Straftaten in Europa, wie Schulter-Surfen[3] oder Taschendiebstähle und Raub besonders bekannt sind. In vielen Fällen sind die Gruppenmitglieder in ihren Heimatländern nicht wegen aktueller Straftaten bekannt, obwohl sie Vorstrafen haben. Durchschnittlich werden zehn MOCG aus jeweils zwei bis vier Personen jährlich verurteilt, wobei fast die Hälfte der verurteilten Mitglieder aus Rumänien stammt. Jede MOCG kann mit 20 bis 30 Straftaten in Verbindung gebracht werden. Die Ausbeute pro Diebstahl beträgt etwa 1.000 bis 1.500 €.

Die Ausführungen über **„The local Dimension in the Containment of international Organised Crime: The Dutch Example"** (**Die lokale Dimension der Eindämmung internationaler OK**) von **Prof. Dr. Cyrille Fijnaut**, Professor für internationales und vergleichendes Strafrecht an der Universität Tilburg in den Niederlanden, konzentrierten sich auf Geschichte, Kontext und Eindämmung der OK in kriminogenen Sektoren, insbesondere im Rahmen des sogenannten Emergo-Projekts,[4] das die Zusammenarbeit von Forschung und Analyse unterstützte, um den Umfang und die Problematik der Organisierten Kriminalität in den Niederlanden und insbesondere in Amsterdam zu beleuchten.

Zunächst verwies Fijnaut auf historische Aspekte der Entwicklung der OK wie das Bandenwesen und die städtischen Unterwelten. Detaillierter wurde das Konzept des internationalen Straftäters dargestellt, der durch die Urbanisierung und das Eisenbahnsystem aus mehreren Ländern heraus tätig sein und neue Sektoren erschließen konnte. Aktuell vollzieht sich eine umfassende Debatte über eine gemeinsame OK-Definition. Einige Experten betonen, dass das Wesen der OK durch die Personen, die für die Bildung krimineller Netzwerke verantwortlich sind, und deren Tatbeitrag geprägt wird. Andere führen aus, dass die begangenen Taten und nicht die Konstellation der beteiligten Personen den OK charakterisieren. Fijnaut skizzierte die Problematik in Bezug auf die Personen und deren Tätigkeiten und führte bezüglich krimineller Aktivitäten aus, dass bei der Lieferung von Waren und Dienstleistungen auf Schwarzmärkten viele Ähnlichkeiten zwischen den EU-Ländern bestehen. Trotzdem gibt es lokale Unterschiede bei der Kontrolle illegaler Märkte.

---

[3] Schulter-Surfen (*shoulder surfing*) ist ein Sicherheitsangriff, der sich mit „über die Schulter schauen" interpretieren lässt und dem Ausspähen von Passwörtern, PIN-Nummern o. Ä. dient, um diese später illegal nutzen zu können (beispielsweise bei der Eingabe an Geldautomaten oder beim Einloggen am PC).

[4] Das Projekt Emergo befasste sich mit der Bekämpfung der Schwerkriminalität in Amsterdam.

Fijnaut kam zu der Bewertung, dass die OK in Amsterdam nicht transnational ist, denn die OK bleibt in der Innenstadt, was auch am Beispiel der La Cosa Nostra in New York veranschaulicht werden konnte. Die transnationale Dimension ergibt sich durch Überschreitung der Grenzen z. B. von Manila nach Amsterdam und der damit verbundenen Notwendigkeit für organisierte Straftäter, ein gutes Kommunikationssystem aufzubauen. Außerdem wies Fijnaut darauf hin, dass „transnationale OK" häufig verwendet werde, um die Auswirkungen der OK darzustellen, die sich nicht ausschließlich auf „traditionelle" OK-Länder wie Italien oder Kolumbien konzentrieren würde. Es sollte nicht nur die transnationale OK-Ebene, sondern auch die lokale Dimension betrachtet werden, denn ohne eine lokale Bekämpfung der OK durch die Behörden ist das Problem auch international nicht einzudämmen. Eine mögliche Methode zur Beherrschung des Problems wurde bereits in den USA und insbesondere in New York genutzt: Sie betrifft die Vergabe und den Entzug von Lizenzen zur Bekämpfung illegaler Märkte. Außerdem bekräftigte Fijnaut, dass die Zuständigkeit bei den lokalen Behörden liege und das New Yorker Beispiel zeige, dass die rechtlichen Möglichkeiten im administrativen Bereich ausgeschöpft werden können. Fijnaut stellte klar, dass nicht nur die aktiv an OK-Straftaten beteiligten Personen, sondern auch die die OK verstärkenden und davon Profitierenden strafrechtlich verfolgt werden sollten. Dies wurde am Beispiel des Philips-Leuchtmittelverkaufs an Personen gezeigt, die aktiv im Anbau von Cannabis tätig waren und damit den illegalen Cannabisanbau intensivierten. Der illegale Cannabisanbau und die Produktion synthetischer Drogen stellen in den Niederlanden das größte Problem dar: Beinahe 3.000 Personen arbeiten täglich im illegalen Cannabisanbau. Dies führte zum nächsten Thema, bei dem sich Fijnaut auf die aktuelle Debatte zur Legalisierung von Cannabis konzentrierte, um das OK-Problem einzudämmen. Einerseits ist die Legalisierung von Cannabis eine profitable Möglichkeit zur Erwirtschaftung von Erträgen und andererseits eine wirksame Maßnahme in der OK-Bekämpfung. Die Niederlande können dies jedoch nicht im Alleingang tun. Es wurde angeregt, dass die Legalisierung von Cannabis unter Umständen auch unter Beteiligung Deutschlands im europäischen Rahmen erfolgen sollte. Außerdem beschrieb Fijnaut spezielle Maßnahmen in Amsterdam, um OK zu definieren, zu reduzieren und einzudämmen. In den Niederlanden besteht dringender Bedarf, neue Maßnahmen zur Bekämpfung der OK zu entwickeln. Zu diesen Maßnahmen zählten auch das Emergo-Projekt, die Einrichtung spezieller Bekämpfungseinheiten und die Durchführung von Projekten im Bereich der Organisierten Kriminalität in Amsterdam durch die Forschungsgruppe Fijnauts, die die „Verflechtung" zwischen OK und legaler Wirtschaft untersuchte. Ein Ansatz bestand darin, die Kontrolle über den Immobilienmarkt zurückzugewinnen. Dies gelang, indem bei der Erteilung von Konzessionen Screenings eingesetzt und die Möglichkeiten für kriminelle Märkte insgesamt reduziert wurden.

Wilbert Paulissen, Chief Superintendent und Leiter der *Central Criminal Investigations Division* in Driebergen, NL, hielt einen Vortrag mit dem Titel **„Countering Outlaw Motorcycle Gangs in the Netherlands"**, der sich auf die Entstehung illegaler Motorradgangs (*Outlaw Motorcycle Gangs*, OMG) und die entsprechenden Maßnahmen und Vorgehensweisen der Behörden zur Bekämpfung dieses Problems konzentrierte.

Zunächst wurden Hintergrund und Datenlage zu OMG präsentiert, denn die OMG in den Niederlanden und Deutschland stehen miteinander in Verbindung. Danach gab Paulissen einen Einblick in die Ziele, Probleme und Vorgehensweisen der *Dutch National Crime Squad* (Niederländische Nationale Verbrechensbekämpfungseinheit, DNR) und der *Dutch National Police* (Nationale Polizei der Niederlande, KLPD). Die DNR bekämpft internationale OK und konzentriert sich derzeit auf die Probleme im Süden der Niederlande, geht gegen Terrorismus vor und ermittelt in Fällen von nationalem Interesse. Am 1. Januar 2013 wurden die bisherigen 25 Länderpolizeien und die niederländische *Police Services Agency* (KLPD) zu einer nationalen Polizei zusammengeschlossen

Nach einer Mordserie in den Niederlanden wurde ein neuer Bekämpfungsansatz entwickelt. Es handelt sich um einen behördenübergreifenden Ansatz, der auf der Überzeugung basiert, dass strafrechtliche Ermittlungsverfahren nicht ausreichen, um internationale OK zu bekämpfen, sondern die Polizeibehörden darüber hinaus mit Kommunen kooperieren und mit Privatunternehmen zusammenarbeiten müssen.

Eine Analyse polizeilicher Informationen ergab, dass Vertreter von neun OMG zwecks Austauschs und Konfliktvermeidung einen Rat gebildet hatten. Dessen Treffen wurden 2013 abgebrochen, als die „Satudarah" aus der Gruppe ausschied. Damals erhoben die Hells Angels den Anspruch, die einzige internationale OMG zu sein, sodass bei den Behörden das Bewusstsein dafür aufkam, dass die Existenz zweier internationaler OMG in einem Land wahrscheinlich einen Krieg unter den Motorradgangs auslösen würde. 2015 erhöhte die „Satudarah" die Zahl ihrer Chapter auf 79 in 90 Ländern und ihre Unterstützergruppen waren ebenfalls deutlich angewachsen. Das Ziel, die Anzahl der Chapter zu verringern, wurde nicht erreicht. Paulissen fasste den Sachstand zu „Satudarah" zusammen und wies darauf hin, dass sie in den ersten 20 Jahren ihres Bestehens keinen großen Zuwachs verzeichnet hatte, dieser nach ihrem Ausscheiden aus dem Rat aber exponentiell anstieg. Außerdem agieren OMG wie „Satudarah" oder „No Surrender" nach Paulissens Ansicht zunehmend medial, um sich in der Gesellschaft zu etablieren. Eine der Vorgehensweisen der niederländischen Polizei beinhaltet daher Kontaktaufnahme, Überprüfung und Befragung der an den Medienauftritten der OMG Beteiligten. Im Zusammenhang mit dem Vorgehen gegen die in den

Niederlanden neu gegründeten „Bandidos", die nur wenige Chapter haben, begannen nationale Polizeibehörden mit regionalen Polizeikräften zusammenzuarbeiten, was zur Verurteilung mehrerer Mitglieder führte und das Wachstum der „Bandidos" in den Niederlanden vorerst stoppte. Die Schließung von Clubhäusern führte zur Bedrohung und Einschüchterung von Beamten und insbesondere Bürgermeistern. Paulissen erklärte, dass es bedeutsam sei, als einheitlicher Akteur vorzugehen, um diesem Problem zu begegnen.

Die Präsentation zu **„Eastern European Cybercrime Groups"** von **Prof. Dr. Federico Varese**, Professor für Kriminologie an der Soziologischen Fakultät des Nuffield College, befasste sich mit zwei Fallstudien zum russischen Cyber-Untergrund. Varese beschrieb seine Exkursion nach Ramnicu Valcea, Hauptstadt des Bezirks Valcea in Rumänien, die als Cybercrime-Hub in Europa gilt. Er wies darauf hin, dass bezüglich der von den UN verfassten Definition der Organisierten Kriminalität große Verwirrung herrscht, da sie zur Entwicklung von Hypothesen zu vage ausfalle. Varese erklärte, vorzugsweise sich als nützlich erwiesene Konzepte der Soziologie, Politologie und Wirtschaftswissenschaften zu gebrauchen, d. h. Produktion, Handel und Governance. Wie in der „legalen" Welt gibt es in der illegalen Welt Personen, die Waren und Dienstleistungen erzeugen. Andere transportieren diese Waren in diverse Städte und Länder, was man normalerweise als Schmuggel bezeichnet. Der dritte Aktivitätstyp wird häufig missverstanden: Personen, die ihre Güter nicht nur verkaufen und transportieren, sondern sammeln, um zu entscheiden, wer produzieren und handeln darf. Varese legte dar, dass dies in der legalen Welt eine staatliche Tätigkeit sei, weil der Staat ein natürliches Monopol über die Ambiguität des Regierens durchzusetzen versuche. Solche Entscheider werden im Allgemeinen vernachlässigt, obwohl sich diese Personen von denjenigen, die in der legalen Welt Produkte herstellen und handeln, deutlich unterscheiden. Bezüglich der Produktion verwies er auf einen Fall von Kokainerzeugung in Kolumbien, bei dem das Kokain in Thunfischdosen verpackt und dann nach Kalabrien transportiert worden war. Dazu wurde eine Kokain-„Marke" entwickelt, um den Ruf der Waren als zentrales Element im Handel aufzubauen. Zur Sicherung der Kooperation würde bei nicht vorhandenem Vertrauen in die Geschäftspartner die Möglichkeit in Betracht gezogen, vorübergehend Geiseln zu nehmen.

Varese machte Ausführungen zur russischen Cybercrime, deren Ausmaß er mittels Bestandsaufnahme und Auswertung der Mitgliedszahlen einschlägiger Foren gemessen hat, und ging von 60 bis 78 Foren mit bis zu 220.000 Nutzern aus. In den Foren werden u. a. Uploads von Schadsoftware, Übernahme von Routern, Attacken auf Mobiltelefone und Geldwäsche im Zusammenhang mit dem Erwerb von Unternehmenskonten in den USA, Deutschland usw. gehandelt. Varese bezeichnete dies insofern als *Bulletproof hosting*, als Websites einen sicheren Server zur Speicherung illegaler Daten offerieren.

Außerdem kann man im Falle von Vertrauensproblemen bei einer Partnerschaft auch Begleitschutz kaufen. Er lenkte die Aufmerksamkeit auf die Tatsache, dass die Preise für derartige Dienstleistungen recht gering seien, was auf einen florierenden Markt hindeute, der vom Forum-Administrator gut verwaltet werde. Angesichts neuer, automatisierter Foren mit standardisierten Dienstleistungen haben sich zudem neue Märkte entwickelt, sodass keine Notwendigkeit mehr besteht, lange Forumsdiskussionen zu führen.

Varese untersuchte auch die Auswirkungen der Ukrainekrise auf die russische Cyberwelt. Die wichtigste Regel der Community lautet anscheinend, die russischsprachige Community nicht anzugreifen. Mit den jüngsten Entwicklungen in der Ukraine ergibt sich daher eine Spaltung in der Community in pro-ukrainische und pro-russische Gruppen. Das ruft Angriffe im russischsprachigen Cyberspace auf den Plan und könnte den „Hacktivismus" verstärken.

In Ramnicu Valcea in Rumänien sieht Varese eine starke lokale Konzentration von Cyber-Tätern, die dort ungestört agieren können. Er verwies darauf, dass bereits unter der Regierung Ceauşescus in IT, Programmierung etc. investiert worden wäre und dies eine lebendige technologieaffine Kultur verstärkt habe. Aber ist Ramnicu Valcea tatsächlich der Knotenpunkt europäischer Cybercrime? Varese beantwortete diese Frage durch einen statistischen Verweis: Die Mehrzahl der Betrugsfälle in Ramnicu Valcea betreffe Kunden aus dem Vereinigten Königreich, die beispielsweise mittels Fake-Angeboten bei eBay dazu gebracht werden, Zahlungen auf ein britisches Bankkonto anzuweisen, von wo es dann von einem Kurier abgehoben und nach Rumänien weitergeleitet werde. Die meisten Betrüger hätten eine spezielle IT-Schule besucht und wurden von ihren Lehrkräften mit diesem Gebiet vertraut gemacht. Die korrupte lokale Verwaltung und die Polizei unterstützen nach Vareses Einschätzung Cybercrime.

In seinem Vortrag **„Corruption Threats in Southern Eastern Europe"** befasste sich **Botschafter Dr. Uglješa Zvekic**, Senior Advisor in der *Global Initiative against Transnational Organized Crime* in Genf, mit Verbindungen zwischen Korruption und OK aus theoretischer bzw. praktischer südosteuropäischer Perspektive.

Zvekic erklärte, dass Korruption eines der Hauptrisiken für die rechtliche, wirtschaftliche und politische Stabilität sei und in der OK als Mittel zur Durchführung illegalen Handels, zur Legalisierung der Erlöse und zur Flucht vor Strafverfolgung genutzt werde, indem beispielsweise in legale Unternehmen investiert werde. Im Kontext zunehmender Kriminalitätsbedrohungen und -risiken sei es bemerkenswert, dass Gewaltkriminalität zurückgehe, während globale OK und Korruption zunehmen. Diese Tendenz fördert eine Zunahme internationaler juristischer Maßnahmen und der Kooperation. Einfüh-

rend analysierte Zvekic, dass Korruption im *Corruption Perceptions Index* (Index der wahrnehmbaren Korruption, CPI) von Transparency International (TI) auf internationaler Ebene anerkannt sei. Zvekic benannte Umfragen von TI und UNODC, um die Anfälligkeit von Institutionen gegenüber Korruption zu illustrieren. Die höchsten Korruptionsniveaus sind demnach in politischen Parteien, öffentlichen Verwaltungen und bei der Polizei zu finden, d. h. in Institutionen, die normalerweise die Kontrolle innehaben und die Ordnung des Systems aufrechterhalten sollen. Zvekic erinnerte daran, dass es sich bereits um reale Bedrohungen handele, die sich in Zukunft noch verstärken dürften, wenn sie nicht entsprechend eingedämmt würden Bestechung in Institutionen bedeutet aber staatliche und gesellschaftliche Schwäche, sodass beispielsweise Polizeireformen wie die Stärkung von Verantwortlichkeiten und die Eindämmung der Korruption erforderlich sind.

OK ist in den Balkanstaaten eher eine Gruppentätigkeit als eine Einzeloperation. Durch den Fall der Berliner Mauer erlebte man auf dem Balkan eine „Wildwest"-Privatisierung, die zur Entwicklung der OK in der „neuen Welt" führte. Einen weiteren Schwerpunkt in der Präsentation Zvekics bildete die Legalisierung krimineller Gewinne, weil das Waschen illegal erwirtschafteter Gelder selbst einen Legalisierungsprozess darstellt. Gleichwohl stehen Maßnahmen zur Bekämpfung der Geldwäsche zur Verfügung. Abschließend erklärte er, dass öffentliche Ausschreibungen und privatisierte Wirtschaft die OK-Ausbreitung auf dem Balkan verstärkt haben: Durch Öffnung des Markts für neue Investitionen kann sich OK legale Präsenz erkaufen. Vor diesem Hintergrund sind die Stärkung der öffentlichen Verwaltung und die Überwachung öffentlicher Ausschreibungen von großer Bedeutung, da die Polizei in der Regel erst einschreitet, wenn eine Straftat begangen ist.

In seiner Präsentation über **„Eurasian Organised Crime Structures in Germany – Countermeasures and Efforts of German Law Enforcement Agencies"** präsentierte Kriminalhauptkommissar **André Schünemann**, M. A., vom Bundeskriminalamt (BKA) in Wiesbaden aktuelle Maßnahmen der deutschen Strafverfolgungsbehörden zur Bekämpfung der Ansiedlung eurasischer OK-Gruppen in Deutschland und insbesondere georgischer Einbrecher sowie Ladendiebe, die unter Aufsicht professioneller Straftäter stehen.

Zunächst wurden grundlegende Informationen zur eurasischen OK betrachtet und anschließend das Projekt JASON vorgestellt, das sich mit georgischen OK-Strukturen befasst. Danach thematisierte Schünemann die Vorgehensweise des BKA bei der OK-Bekämpfung. Die „Diebe im Gesetz", bei denen es sich in erster Linie um Berufsverbrecher handelt, stehen an der Spitze der Hierarchie der russisch-eurasischen OK. Die Situation in Deutschland wurde im Zusammenhang mit der Größe der hiesigen russischsprachigen Bevölkerung (4,5 Millionen Menschen) illustriert. Etwa 4.500 bis 5.500 Insassen von

Justizvollzugsanstalten unterwerfen sich dem Kodex der „Diebe im Gesetz" in Deutschland. Russisch-eurasische OK-Gruppen bleiben für Bürger und mitunter auch Polizei unsichtbar, sofern ihre kriminellen Aktivitäten nicht öffentlich werden. Deliktsbereiche georgischer OK-Gruppen wie Eigentumsdelikte, Betrug, Geldwäsche und Investitionen in legale Unternehmen veranschaulichte Schünemann anhand von Beispielen. Schwierigkeiten bestehen darin, die Verbindung zwischen georgischen Ladendieben und kriminellen Strukturen der russisch-eurasischen OK nachzuweisen. Berichte aus mehreren Bundesländern belegen, dass in Deutschland als Asylsuchende registrierte georgische Staatsbürger in diesen Kriminalitätsbereichen tätig sind. Im Rahmen des Projekts JASON hat sich das BKA zur Aufgabe gemacht, auf nationaler Ebene Maßnahmen gegen georgische OK-Gruppen einzuleiten, um georgische OK-Strukturen und -Logistik zu zerschlagen und Beweise, dass georgische Kleinkriminelle von den „Dieben im Gesetz" geführt werden, zu sichern. Weiterhin soll in nationales Netzwerk zur Kriminalitätsbekämpfung etabliert und die internationale Kooperation verstärkt werden. Bei der nationalen und auch internationalen Koordination sind Europol, Interpol und die Behörden der von georgischer OK betroffenen Länder wichtige Partner.

Ein weiterer Schwerpunkt des Vortrags lag auf dem Projekt MILLENNIUM, einer Kooperation zwischen Interpol und 45 Mitgliedsländern zur Erhebung und Verarbeitung von Informationen zur russisch-eurasischen OK. Deutschland unterstützt und fördert das Projekt als Mitinitiator. Angesichts neuer Kriminalitätsphänomene sind auf Analyse- und Ermittlungsprojekten basierende Konzepte zur OK-Bekämpfung notwendig. So wurde im BKA eine OK-Koordinationsstelle eingerichtet, die vierteljährlich aktuelle OK-Arbeitsschwerpunkte in Bund und Ländern abfragt, die Zusammenarbeit der betroffenen Stellen koordiniert und die Kommunikation national und international stärkt. Schünemann erläuterte, wie gemeinsame Arbeitsschwerpunkte identifiziert werden können und welche Perspektiven das Projekt JASON für die künftige Kriminalitätsbekämpfungsarbeit bietet.

Ausblick

Zurzeit wird versucht, EU-Gelder für ein weiteres Folgeprojekt zu beantragen. Im Jahr 2016 wird jedoch keine Forschungskonferenz stattfinden. Es wird angestrebt, das OK-Forschungsnetzwerk aufrechtzuerhalten und auch künftig Fachkonferenzen zum Thema „Transnationale Organisierte Kriminalität" auszurichten. Auch in Zukunft sollen Veranstaltungen zu ausgewählten phänomenologischen Schwerpunkten mit internationalen Bezügen durchgeführt werden.

Part VI

List of contributors

Prof. Dr. Cyrille Fijnaut

Professor of International and Comparative Criminal Law, Tilburg University, Tilburg, The Netherlands

Dr. hab. Wojciech Filipkowski

Professor of the University of Bialystok, Faculty of Law and Head of the Forensic Science Laboratory, University of Bialystok, Poland

Michael Hay

Researcher at the Organised and Cyber Crime Research & Analyses, Home *Office*, United Kingdom

Mary Hess

Freelance translator, Mainz-Kastel, Germany

Edwin Kruisbergen, MA

Researcher at the Research and Documentation Centre at the Ministry of Security and Justice, The Hague, The Netherlands

Johan Lundberg

Superintendent, Swedish Police Authority, Police Region West, Gothenburg, Sweden

Fredrik Mattsson

Tactical analyst and criminologist at the National Operational Department, Stockholm, Swedish Police

Kim Nilvall

Detective Inspector, Swedish National Bureau of Investigation, Swedish Police, Stockholm, Sweden

Dr. Szilveszter Póczik

Project Manager and Senior Researcher at the National Institute for Criminology, Budapest, Hungary

Bradley Schmidt

Freelance translator and editor, Leipzig, Germany

André Schünemann, MA

Kriminalhauptkommissar, Bundeskriminalamt, Wiesbaden, Germany

Dr. Louise Shelley

Director, Terrorism, Transnational Crime and Corruption Center (TraCCC), University Professor, School of Policy, Government and International Affairs, George Mason-University, Fairfax, United States

Dr. Gavin Slade

Criminologist, Research Fellow, Free University Berlin, Dahlem Research School, Germany

Prof. Dr. Federico Varese

Professor of Criminology, University of Oxford, Nuffield College, Oxford, United Kingdom

Daniel Vesterhav

Head of Division for Research on Economic and Organised Crime of the Swedish National Council for Crime Prevention (Brå), Sweden

Julia Weber

Student of Sociology and American Studies at Goethe-University Frankfurt, Germany

Benedikt Welfens

Senior Public Prosecutor, Deputy to the National Member for Germany, Chair of the Team Trafficking and Related Crimes, EUROJUST, The Hague, The Netherlands

Martin Zimmermann

Freelance editor, Magdeburg, Germany

Ambassador Dr. Ugljesa Ugi Zvekic

Senior Advisor, Global Initiative against Transnational Organized Crime, Geneva, Switzerland

About the editors and the authors

Editors

Ursula Töttel is a CID officer (Kriminalhauptkommissarin) at the Bundeskriminalamt Wiesbaden. She worked as a police officer in the area of terrorism, especially fugitive searches, in the surveillance group and overseas contacts and participated in several special inquiry teams following terrorist attacks. For eight years she worked in the field of analysis and evaluation in organised drug crime. Since 2007, she has been part of the Research and Advisory Unit for Organised and Economic Crime and Crime Prevention and project leader of the EU project Research Network on Organised Crime.

Dr. Gergana Bulanova-Hristova is a political scientist, working since 2011 as researcher at the Research and Advisory Unit for Organised and Economic Crime and Crime Prevention of the Bundeskriminalamt, Wiesbaden. After finishing her studies in international relations at the University for National and World Economy in Sofia 2002 and in political science at the Free University in Berlin 2006, she was a doctoral fellow at the Free University in Berlin and a doctoral grant-holder from the Friedrich-Ebert-Foundation. Before joining the Bundeskriminalamt she was a research assistant at the Free University in Berlin and worked as process optimizing advisor at T-Systems-International Ltd. Her research interest and expertise include countering of corruption, organised crime and good governance.

Gerhard Flach is a CID officer (Erster Kriminalhauptkommissar) in the Research and Advisory Unit for Organised Crime, Economic Crime and Crime Prevention at the Bundeskriminalamt. His tasks include the planning and carrying out of research projects in the field of organised crime. He was previously Lecturer in Criminalistics at the Academy for Police Officers, CID section of the Federal College of Public Administration and worked as investigator in countering national and international terrorism and organised crime.

Authors

Prof. em. Dr. Cyrille Fijnaut is Professor of International and Comparative Criminal Law at Tilburg University in the Netherlands. Before starting his academic career, he studied at the Dutch Police Academy and worked as a police lieutenant in the police force of the city of Tilburg. He then began to study criminology and philosophy at the KU Leuven and defended his PhD-thesis on the political history of the police systems in North-West Europe. He was Professor of Criminology and Criminal Law at various universities in

Belgium and the Netherlands. His main research interests are related to organised crime, terrorism and social safety, international police and judicial operation, the history of policing in Europe, comparative criminal procedure and police law as well as the development of European and American criminology. He published various articles in national and international journals and edited many books. Moreover, he served as an expert for a number of governmental and parliamentary committees of inquiry in the Netherlands with reference to organised crime problems. He currently dedicates most of his time to two books he is working on.

Dr. hab. Wojciech Filipkowski, is a Professor at the University of Białystok, Poland, holds a degree in legal science and is the Head of the Forensic Science Laboratory at the Faculty of Law of the University of Białystok as well as the Director for Scientific Matters of the European Institute of Homeland Security. Moreover, he is the author of over 100 publications in Polish and English in the field of criminology, forensics, and substantive criminal law as well as an expert in the field of money laundering and financing of terrorism. Currently, he specializes in legal, criminological, and forensic-science aspects of the use of modern technologies, in particular information and communication technologies, by law enforcement agencies and the judiciary in order to fight crime including organised and economic crimes. Since 2006, he has participated in over 11 domestic and scientific research and development projects in the field of broadly defined security, including projects lead by technical universities. In the years 2009–2011, he was the manager of the R&D project titled "Legal and criminological aspects of implementation and use of modern technologies aimed to protect internal security," financed by the National Centre for Research and Development. He is also a member of the Prof. Stanisław Batawia Polish Criminological Society and of the Polish Platform for Homeland Security.

Johan Lundberg is a Superintendent at the Swedish Police Authority in the Police Region West in Gothenburg, Sweden. He started his apprenticeship in 1988 and worked then as a police officer at the Hudding Police Department as well as in the Skovde Police Department. In 2006, he became Superintendent and Chief of the Local Police District Vastra Skaraborg and operated as head of various projects concerning organized crime for instance the project for a safer city and project metal thefts. Moreover, since 2007, he led various training courses such as project leading at the high-school in Jonkoping or the Leadership training at Lund University. In 2011, he became Chief Superintendent at the Police District Skaraborg and in 2014, he acted as project manager and Chief at the Region Office West.

Stefan Michel is Leitender Kriminaldirektor and Deputy Head of the Division Serious and Organised Crime at the Bundeskriminalamt in Germany.

Kim Nilvall is a Detective Inspector at the Swedish National Bureau of Investigation, Swedish Police, Stockholm. He started as an interrogator at the unit for serious crimes in Gothenburg, 1995 and continued to work as an investigator. In 2002, he became a project manager within NCIS Sweden and lead the projects XTC and Internet related drug trafficking. He cooperated from 2005 till 2010 with Interpol in the "Project drugs.net" and worked in several countries in overseas and Eastern Europe. Since 2010, he has conducted analytical trainings on the "Criminal Arboristic Approach" in in places including Nicaragua and Serbia. He developed a methodology regarding the strategic recruitment of informants and was responsible for the National Drug Threat Assessment. In 2013, he worked as cooperative party with the Ministry of Security of the Republic of Chine within New Psychoactive Substances. Since 2014, he has been responsible for the Swedish part within the Dutch project ITOM. Furthermore, he has published a number of reports, for example an analysis of consequences for police work in relation to the new praxis stated by the Supreme Court in Sweden regarding penalty degree in drug related crimes.

Fredrik Mattsson is a tactical analyst and criminologist at the Swedish police, National Operational Department, Stockholm. He started as investigator, between 2001 and 2004, at The Swedish National Council for Crime Prevention, mainly with questions regarding crime prevention from a local point of view. He started to work at The National Bureau of Investigation in 2004, with both operational and strategic analysis mainly concerning Outlaw Motorcycle-Gangs, cash in transit robberies and different kinds of violent crimes. Since 2010, he has conducted analytical trainings on "The Criminal Arboristic Approach" in i. e. Sweden, Norway and Serbia. Further, he has published and been the editor for a number of reports, for example the Swedish police annual tactical report, "Strategic persons within organized crime", "Serious robberies – Mapping and analysis of legal and methodological issues" and "Threat to people in the justice chain. A draft for a national action plan".

Dr. Szilveszter Póczik, is a Project Manager at the National Institute of Criminology (NIC), in Budapest. He studied modern history, social sciences and linguistics in Debrecen, Hungary, and in Greifswald, Germany. Supported by the scholarship of the Hanns Seidel Foundation he was guest researcher in the Institute of Contemporary History in Munich for three years. He acquired his PhD degree on the historical theories on fascist movements and dictatorships in 1992 and continued teaching at the university as lecturer until 2002. In 1994, he was invited by the National Institute of Criminology to lead a research project and was employed as senior researcher. He took part in several advanced trainings and won numerous prices and scholarships. Since 1994, he has devoted himself to criminology. He deals with crime of social and ethnic minorities and immigration groups, xenophobia, racism, political extre-

mism, terrorism and organised crime. He is author and editor of monographs and numerous studies. Since 2006 he is the Chairman of the ATKA Public Interest Foundation for Applied Social Researches.

André Schünemann is a CID officer in Germany. He worked in different areas in fighting organised crimes in Germany and was deployed to Southeastern Europe for four years. He completed a MA degree in Criminal Justice, Governance, and Police Science and is an expert on transnational organised crimes.

Prof. Dr. Louise Shelley is not only the Omer L. and Nancy Hirst Endowed Chair, but also the founder and director of the Terrorism, transnational Crime and Corruption Center (TraCCC) at George Mason University in Fairfax. She was an inaugural Andrew Carnegie Fellow in 2015 and she is presently working on her book "Illicit Trade: Global Challenge" for Princeton UP which examines the impact of illicit trade on the sustainability of the planet. Moreover, she has edited books and written dozens of articles on transnational crime and corruption. For six years, she served as a member of the WEF and was the initial co-chair of the global agenda council on organized crime. She also is a member of the Global Initiative against Transnational Organized Crime and a life member of the Council of Foreign Relations. In addition, she won a number of prizes and fellowships such as the Guggenheim and two Fulbright fellowships for research in the Soviet Union. Her main fields of interest are post-Soviet OC, money laundering, human trafficking and illicit wildlife trade and she repeatedly addresses fora on these topics.

Dr. Gavin Slade is a Criminologist and Research Fellow at the Free University Berlin and Dahlem Research School. He received a doctoral degree in criminology from the University of Oxford and has extensive experience researching organised crime in the post-Soviet region, writing many academic articles on issues of crime and corruption in this region. He has published a book with Oxford University Press on the success of the anti-mafia campaign in the republic of Georgia and the dynamics of the groups that it targeted. From 2012–2014, Slade was Assistant Professor of Criminology at the University of Toronto, Canada. In 2014, Slade won a research fellowship at the Free University, Berlin to study anti-organized crime policy and its connection to prison reform in Eurasia.

Prof. Dr. Federico Varese is Professor of Criminology at the University of Oxford, where he joined the faculty in 2003. Before obtaining the title of Professor of Criminology in 2006, he was Assistant Professor of Sociology at Williams College and William H. Orrick Visiting Professor at Yale University. Furthermore, he was a Prize Research Fellow at Nuffield College where he obtained a D. Phil. in Sociology in 1997. He also holds degree in Political Science from Bologna University and an M. Phil. in Social and Political The-

ory from King's College, Cambridge. His main research interests are the study of organised crime, corruption, Soviet criminal history and the dynamic of altruistic behaviour. Currently, he works on the application of network analysis to criminal behaviour and the rescue of persecuted minorities during the Nazi occupation of Europe. He has published various articles in well-known academic journals such as *Law and Society review* and is himself editor of the *Global Crime* journal. *The Russian Mafia*, his book from 2001, won the Ed Hewitt Prize of the American Association for the Advancement of Slavic Studies in 2002.

Benedict Welfens is a Senior Public Prosecutor and Deputy to the National Member of Germany as well as a member in the chair of the Team Trafficking and Related Crimes at Eurojust in The Hague. He holds a diploma in Law with a first and second state examination at the University Saarbrücken since 1991 and became Public Prosecutor at the PPO, prosecuting crimes in the field of juvenile delinquency and white collar crime, in Cologne and Cottbus one year later. In 1997, he was appointed prosecutor at the General Prosecution Office in Brandenburg, which are occupied with the internal control of the PPOs in Brandenburg and prepare mercy decisions as well as investigating lawyers. From 1998 to 2006 he was Senior Public Prosecutor at the PPO in Potsdam and the Head of division of organised crime, serious economic crime and the speaker of the PPO Potsdam which marks a contact point for confiscation of illegal profits for Brandenburg. Since 2006 he has been a Deputy National Member for Germany at Eurojust and coordinates investigations and prosecutions between German judicial authorities and EU-member states.

Ambassador Dr. Ugljesa Zvekic is Senior Advisor at the Global Initiative against Transnational Organized Crime in Geneva, Switzerland. He holds a law degree (LL.B), an MA and PhD in sociology and law. He was a country representative in the UN-sponsored World Youth Forums in 1969 and a Fulbright Scholar from 1973–1975. His main career positions include being an Honorary Professor at the University of Hull, a Deputy Director at the United Nations Interregional Crime and Justice Research in Rome, a Deputy Representative at the UNODC in South Africa, in addition to being the Chief of the Strategic Planning Unit of the UNODC in Vienna. Moreover, he was a permanent representative of the Republic of Serbia to the UN in Geneva as well as consultant at the UNODC/UNITAR/ISICS/IP. Currently, he is senior advisor at the Global Initiative against Transnational OC and visiting professor at the Law School at the University of Belgrade, but also at the University of Governance and the Law School in Rome. His topics of interest include multilateral diplomacy, international crime, global corruption, criminal justice and security reforms as well as geopolitics and political management.

Polizei+Forschung

Content

Since 2008 the yearly research conferences in Germany focusing on organised crime have established a European-wide forum that enables international exchange between academics and practitioners from law enforcement agencies. The event is hosted each year by the Bundeskriminalamt together with its research partners of the "Research Network on Organised Crime" from the United Kingdom, Sweden and the Netherlands. To date, there have been participants from 23 European countries and the United States. The conferences have received financial support from the EU since 2010.

This book entails summaries of the speeches hold on the conferences from 2013 until 2015 and contributions from the speakers on selected topics in the field of organised crime.

Zum Inhalt

Die jährlichen Forschungskonferenzen in Deutschland zum Thema Organisierte Kriminalität haben in den Jahren von 2008 bis 2015 ein anerkanntes Forum für den internationalen Austausch zwischen Wissenschaftlern und Praktikern aus Strafverfolgungsbehörden geschaffen. Die Tagungen wurden durch das BKA in Zusammenarbeit mit den Partnern aus dem „Research Network on Organised Crime" aus dem Vereinigten Königreich, Schweden und den Niederlanden ausgerichtet und seit 2010 von der EU unterstützt. Auf den Konferenzen waren Teilnehmer aus insgesamt 23 europäischen Ländern und den USA vertreten.

Dieser Sammelband enthält Zusammenfassungen der Einzelvorträge der OK-Forschungskonferenzen von 2013 bis 2015 sowie Beiträge der Redner zu ausgewählten Themen aus dem Bereich der Organisierten Kriminalität.