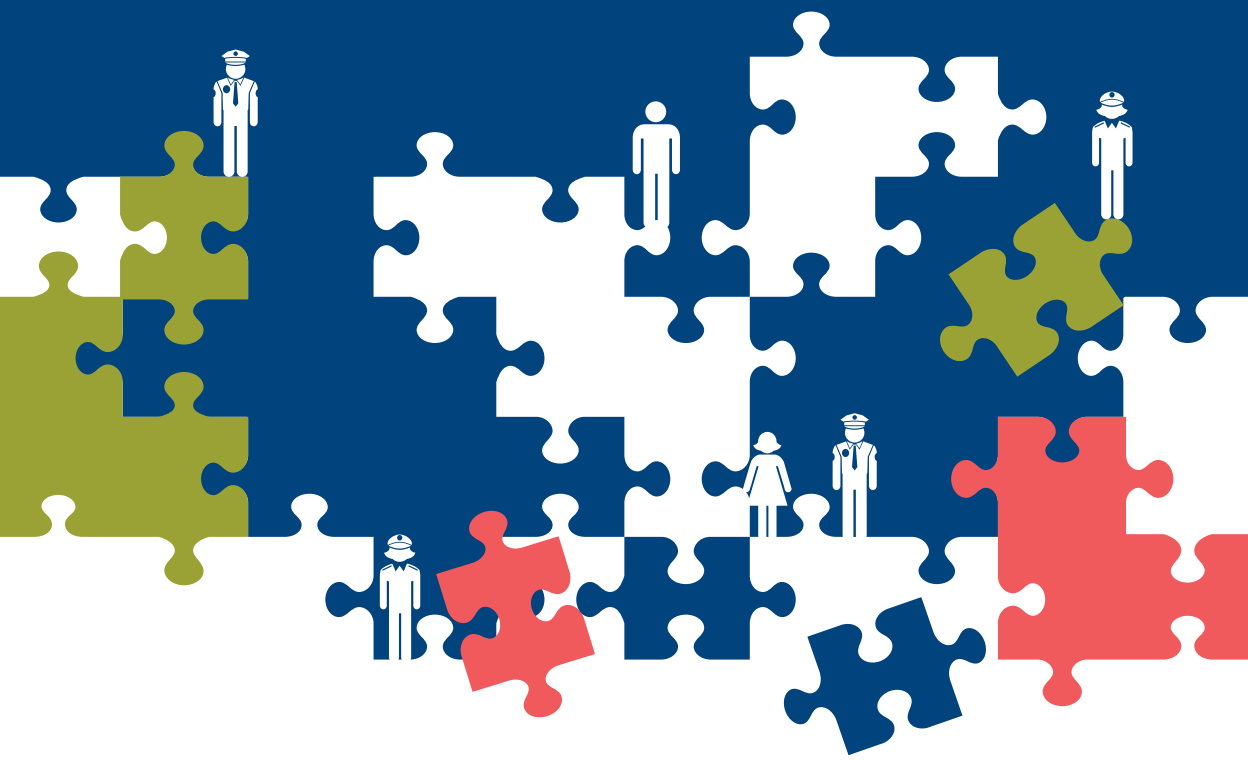
TNTD/SPMU Publication Series Vol. 13

OSCE Guidebook
Intelligence-Led Policing



Organization for Security and Co-operation in Europe

Vienna, June 2017
© OSCE 2017

All rights reserved. The contents of this publication may be freely used and copied for educational and other non-commercial purposes, provided that any such reproduction be accompanied by an acknowledgement of the OSCE as the source.

ISBN 978-3-903128-04-0

OSCE Secretariat
Transnational Threats Department
Strategic Police Matters Unit

Wallnerstrasse 6
A-1010 Vienna, Austria
Tel: +43-1 514 36 6942
E-mail: spmu@osce.org
osce.org/secretariat/policing
polis.osce.org

OSCE Guidebook

Intelligence-Led Policing

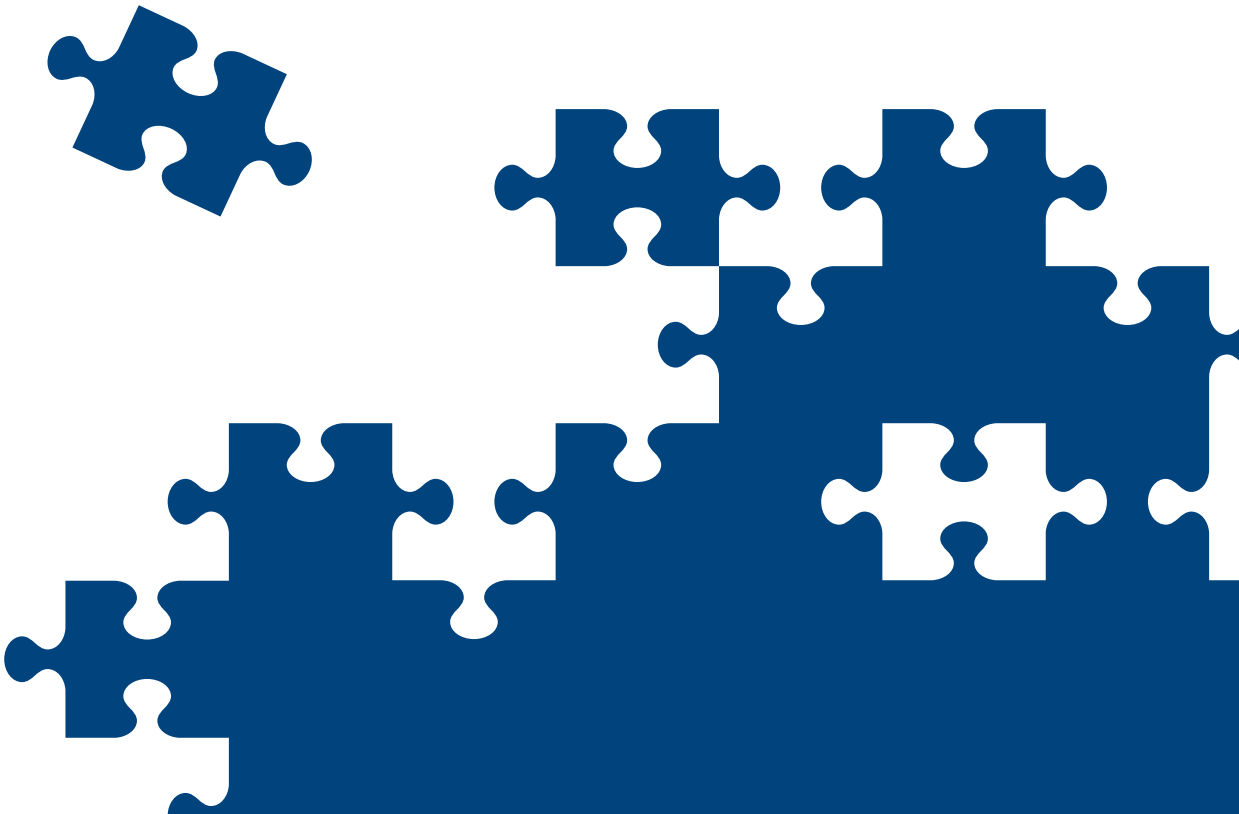


Table of Contents

Preface

Police-related activities are a key element of the OSCE's efforts to strengthen security and stability in the OSCE area and represent an important aspect of the Organization's contribution to strengthening participating States' efforts to address threats posed by criminal activity. Since 1999, police-related activities have been one of the basic components of the OSCE's endeavours in the fields of conflict prevention, crisis management and post-conflict rehabilitation.

In line with its mandate, the OSCE steadily strives to support its participating States in enhancing their competencies, improving the effectiveness of their criminal justice systems, and increasing the capabilities of their law enforcement and police services. The evolution of transnational threats, ever-changing criminal patterns and increasing demand for services provided by the police call for a constant renewal of strategies, priorities, plans and methods. The OSCE Guidebook on Intelligence-Led Policing is an important step by the OSCE towards addressing these challenges.

This guidebook presents intelligence-led policing (ILP) as a modern and proactive law enforcement model, and a realistic alternative to traditionally reactive forms of policing for OSCE participating States. ILP, which has already been adopted in a number of countries in recent years with promising results, combines intelligence gathering, evaluation and analysis with informed decision-making procedures and mechanisms, thus providing more efficient and effective management of national law enforcement.

Research has revealed that ILP has significant potential as a modern law enforcement model, but its success greatly depends on specific requirements, which are outlined in the guidebook. Political support and senior managerial awareness and commitment are among the key prerequisites.

I would like to express my gratitude to more than 30 law enforcement experts from OSCE participating States, academia, international organizations and OSCE field operations who assisted the Strategic Police Matters Unit of the OSCE Transnational Threats Department in developing this guidebook by providing valuable input and reviewing drafts. I would also like to thank our colleagues at the OSCE Office for Democratic Institutions and Human Rights for sharing their expertise on human rights and data protection relevant to ILP and its implementation.

The 2016 German and the 2017 Austrian OSCE Chairmanships have strongly supported the ILP initiative within the OSCE. The publication of this guidebook would not have been possible without their support.

Lamberto Zannier
OSCE Secretary General

Today's law enforcement is facing more complex challenges than ever before. At the same time, public demands for greater effectiveness, efficiency and accountability of the police have been raised considerably. Intelligence-led policing (ILP) developed in recent years as a response to these growing challenges. The model not only provides a modern approach to identifying and planning countermeasures against increased transnational threats such as terrorism and organized crime, but can also be applied to day-to-day proactive planning and police management. At a time of austerity measures and budget constraints, ILP provides law enforcement management with methods and tools to identify priorities and allocate resources accordingly.

This guidebook addresses ILP from four main standpoints. First, it defines ILP and the rationale for promoting the model as a contemporary law enforcement approach, applicable to the OSCE area as a whole. Second, it covers the important subjects of human rights and data protection when implementing ILP. Third, it addresses the analysis of data and information, resulting in strategic and operational intelligence products being used as basis for informed and evidence-based decision-making. Fourth and finally, the guidebook introduces practical recommendations of national, regional and local organizational structures as well as the minimum standards needed for criminal intelligence departments and decision-making mechanisms.

ILP puts criminal intelligence analysis at the core of law enforcement. It also moves criminal analysis and decision-making closer together than other contemporary policing models, calling for new skills and competencies of law enforcement analysts and managers.

The main objective of this guidebook is to provide OSCE participating States with tools to strengthen their law enforcement's professionalism, enhance quality and effectiveness of their activities, and maximize management of their resources, resulting in increased public trust and targeted measures against threats to public security and safety.

Rasa Ostrauskaite
Co-ordinator of Activities to Address
Transnational Threats,
OSCE Secretariat

Executive Summary

Intelligence-led policing (ILP) is a modern approach to law enforcement. First introduced in the United Kingdom in the 1990s, ILP has primarily been used in countering serious and organized crime. Promising results in recent years have prompted law enforcement authorities to expand the intelligence-led proactive methodology to all areas of police management as a comprehensive business model. ILP focuses on systematic gathering and evaluation of data and information, through a defined analysis process, turning it into strategic and operational analysis products, which serve as basis for improved, informed and evidence-based decision-making.

Two of the main challenges of today's law enforcement are the ever-increasing complexities and transnational nature of crime as well as enhanced public demand for financial efficiency, i.e. 'to do more for less'. The ILP model addresses these challenges by emphasizing and providing for intelligence-based prioritization followed by tasking and allocation of available resources in line with defined priorities.

By outlining clear and defined criminal intelligence mechanisms, decision-making procedures and organizational structures at the local, regional and national levels, this guidebook not only presents the conceptual ILP model, but also offers pragmatic tools to implement it. These include day-to-day policing practice, proactive strategic planning and operational action plans as well as instruments to address serious and organized crime. Furthermore, this guidebook explains how ILP can considerably complement community policing while proving an effective tool in countering terrorism, violent extremism and radicalization that can lead to terrorism (VERLT).

Criminal intelligence analysis is given more significance in ILP than other contemporary policing models. This calls for enhanced and sometimes new analytical skills and competencies within the law enforcement. The proactive, forward-looking focus of ILP also relies on law enforcement managers to know how to work with analysts and make use of analytical products in their decision-making and planning. Thus, in adopting and implementing ILP, there must be specific focus on preparing and training high- and middle-level leadership and management within the law enforcement.

Research has revealed that if ILP is to be implemented to its full potential, political support and high- and middle-level management awareness and commitment are vital. Other important preconditions for the successful application of ILP are covered in the guidebook, including: multi-agency approach to law enforcement; clear tasking mechanisms; the transformation of the 'need to know' culture into the 'need to share'; the presence of IT communication channels to forward information; analytical databases and skilled analysts; and relevant organizational structures that support ILP.

For ILP to work effectively, feedback on and evaluation of intelligence products, as well as constant managerial monitoring and quality control of the model are of fundamental importance and must be embedded into its practices.

The absolute obligation of all law enforcement to respect and adhere to human rights and data protection principles while implementing ILP is repeatedly stressed in this guidebook. The gathering, processing and use of data and information must at all times strictly comply with national laws and international human rights standards. With internal and external control mechanisms, and its evidence-based and transparent decision-making procedures, ILP is intended to enhance the accountability of law enforcement management.

This guidebook provides a general framework for ILP and its implementation for the whole OSCE area. Technical details on implementing ILP are not covered, thereby leaving room for OSCE participating States to adapt the model to their respective national needs and circumstances in line with their national legal frameworks.

Acknowledgements

The OSCE Transnational Threats Department would like to thank Arnar Jensson, the Project Manager of this guidebook for his contribution to the development and drafting of this publication. A group of distinguished police experts comprising representatives from OSCE participating States, relevant regional and international organizations, independent research organizations and OSCE executive structures contributed to the guidebook with written inputs and taking part in a two-day draft review experts meeting in Vienna. TNTD/SPMU acknowledges and appreciates the highly valued advice and contributions provided by the following individuals to the drafting process of the guidebook:

Georgi Aladashavili, Chief of Tbilisi Police, Georgia
Roberto Arcieri, Acting Chief of Studies and Research Department, Evaluation and Formation Office, Italy
Leena Anonius, Gender Adviser, Gender Section, OSCE Secretariat
Pero Bozovic, Head of Department for Intelligence, Information Gathering / State Investigation and Protection Agency, Bosnia and Herzegovina
Maryse Chureau, Strategic Analyst / Europol Strategic Analysis Team, Europol
Anders Danielsson, Police Affairs Officer, TNTD/SPMU, OSCE Secretariat
Lotta Ekvall, Adviser on Gender Issues, Gender Section, OSCE Secretariat
Nino Gakharia, Head of Euro Atlantic Integration Division, Ministry of Internal Affairs, Georgia
John Gustavsson, Senior Organized Crime Adviser, OSCE Mission in Kosovo
Johannes Heiler, Adviser on Anti-Terrorism Issues, Human Rights Department, ODIHR
Jesus Hernandez Alvarez, Analyst, National Police, Spain
Iris Hutter, Operational and Strategic Criminal Analysis Unit, Federal Criminal Police, Austria
Adrian James, Senior Lecturer in Criminal Investigation, Institute of Criminal Justice Studies, University of Portsmouth
Erik Johansen, Police Advisor, Civilian Planning & Conduct Capability, European External Action Service
Ivan Jokić, Chief Inspector / Department of Criminal Intelligence, Police Directorate, Montenegro
Maxim Klepov, Ministry of Interior, Russian Federation
Nenad Kostadinović, Deputy Head of ILP Department, Ministry of Interior, Republic of Serbia

Dejan Lazaroski, Head of Strategic Intelligence Unit, Department for Criminal Intelligence and Analysis, Bureau for Public Security, the former Yugoslav Republic of Macedonia
Andrei Muntean, Senior Programme Officer, Office of the Co-ordinator of OSCE Economic and Environmental Activities, OSCE Secretariat
Susanna Naltakyan, National Pogramme Officer, OSCE Office in Yerevan
Tarik Ndifi, Analyst and Researcher, Conflict Prevention Centre, OSCE Secretariat
Marua O'Sullivan, Police Adviser, Public Safety and Community Outreach Department, OSCE Mission to Skopje
Seda Öz Yildiz, Director, Institute of Security Sciences, Police Academy, Turkey
Hans-Juergen Pechtl, Assistant Director, Criminal Analysis Sub-Directorate, INTERPOL General Secretariat, Lyon, France
Mark Reber, Senior Police Adviser, International Association of Chiefs of Police
Joerg Rosemann, Chief Superintendent, Directorate Criminal Investigation, District Police Authority of the Rheinisch Bergischer Kreis region, Northrhine-Westphalia, Germany
Matej Seljak, Criminal Police Directorate, General Police Directorate, Slovenia
Bjordi Shehu, Specialist / Analyst, Directorate of Analysis and Criminal Information, General Directorate of Serious and Organized Crime, State Police, Albania
Simon Smith, Chief Inspector, National Counter Terrorism Policing HQ, Head of Prevent Delivery, United Kingdom
Thorsten Stodiek, Deputy Head of TNTD/SPMU, OSCE Secretariat
Marco Teixeira, Programme Officer, Implementation Support Section, Organized Crime and Illicit Trafficking Branch, Division for Treaty Affairs, UNODC
Adriana Toston Diez, Captain, Guardia Civil, Spain
Per Wadhed, National Operations Department, Swedish Police
Dr. Ireen Winter, Head, Operational and Strategic Criminal Analysis Unit, Federal Criminal Police, Austria
Maica Wurmboeck, Project Assistant, TNTD/SPMU, OSCE Secretariat

Introduction

Background and rationale

Traditional reactive law enforcement models have encountered severe difficulties in coping with today's risks and threats, and reacting to new criminal opportunities caused by, *inter alia*, an increase in personal mobility and migration, rapid technological and communication changes, free movement of goods and services, and growing income inequality. Violent extremism and radicalization that lead to terrorism (VERLT) as well as terrorist incidents in recent years have highlighted the need to share, connect and centrally analyse relevant data and information (intelligence) from all levels, in compliance with national legislations, international human rights standards and OSCE commitments. Intelligence-led policing (ILP) developed as a response to these growing challenges by inspiring and facilitating a *proactive* policing approach, complementing the traditional, *reactive* policing model. It has proved to be an effective tool to address organized crime, to make better use of resources, and to identify and address priority tasks in a targeted manner. The proactive and future-oriented approach of ILP facilitates crime prevention, reduction, disruption and dismantling. Key to the ILP approach is the systematic gathering and analysis of information and data relevant to the prevention, reduction and dismantling of crime, followed by the development of intelligence reports. On this basis, informed and forward-looking policy-making and managerial decisions can be made and resources allocated, addressing the most pressing security concerns, threats, crime types and criminals. ILP has furthermore proved to be an effective and sustainable tool for countering terrorism and VERLT.

Based on its mandate to provide assistance to participating States in building capacity, improving professionalism, and supporting police development and reform, including by developing guidelines[1], the Transnational Threats Department's Strategic Police Matters Unit (TNTD/SPMU) developed this guidebook, *Intelligence-led Policing*. The drafting of this guidebook is a follow-up to the 2016 Annual Police Experts Meeting (APEM), held in Vienna on 9-10 June 2016, where ILP was the subject matter. One of the APEM's Key Findings and Outcomes was the need for a common OSCE notion of the ILP concept and to develop a guidebook for OSCE participating States on the subject. The 2016 OSCE German Chairmanship, the 2017 OSCE Austrian Chairmanship and the OSCE Secretary General have clearly expressed their strong interest and support for further promoting the ILP concept and its implementation, starting with tasking the TNTD/SPMU to draft an OSCE ILP guidebook.

In preparing and drafting this guidebook, particular attention was paid to avoid duplication of efforts and build on work already on the subject by national authorities of OSCE participating States as well as regional and international organizations. Therefore, written material was gathered for this guidebook, with the kind permission from relevant stakeholders. The ILP material

1 OSCE Permanent Council, Decision No. 1049. "OSCE Strategic Framework for Police-Related Activities" (PC.DEC/1049, Vienna, 26 July 2012).

in this guidebook includes and builds on the work of the United Nations Office on Drugs and Crime (UNODC), the United Nations Department of Peacekeeping Operations (UNDPKO), INTERPOL, the European Union External Action Service and Europol.

ILP-related legal documents, formal instructions, national handbooks and other written inputs were gathered from a number of national authorities of OSCE participating States and OSCE field operations. The joint OSCE/UNODC ILP information sheet, issued in April 2016 for the 2016 OSCE Annual Police Experts Meeting (APEM), served as a basis for the OSCE ILP model, which is presented in sub-chapter 7.1 as the proposed framework for implementing the ILP concept in OSCE participating States.

All OSCE participating States and OSCE executive structures as well as a number of regional and international organizations were invited to nominate experts to review drafts and provide inputs to this guidebook. Around 30 nominated experts participated in a two-day draft review workshop in Vienna in December 2016, 15 of whom provided written inputs throughout the drafting process of this guidebook.

The theoretical framework for the OSCE ILP model recommended in sub-chapter 7.1 is based on Professor Jerry H. Ratcliffe's academic research presented in his 2016 book *Intelligence-Led Policing*.[2] Professor Ratcliffe is the most frequently cited scholar on this subject. Three internationally recognized academics presented and introduced their research on ILP-related subjects at the 2016 OSCE APEM.[3] Dr. Adrian James participated in the draft review workshop and provided his written input and academic view on the content throughout the drafting process of the guidebook.

In the process of establishing a common OSCE notion of ILP, linguistic challenges had to be overcome, because intelligence does not convey the same meaning in different languages. The translation of the ILP concept, for instance from English to Russian, can cause some disharmony. The word *intelligence* is commonly understood in Russian as restricted data and information held by security services and other authorized agencies including authorized (responsible) police units, whereas in English, intelligence stands for all kinds of analysed data and information, developed by and accessible to law enforcement agencies. It is important to keep this language disharmony in mind when referring to ILP and to note that, throughout this guidebook, *intelligence* refers to the latter meaning of the word, namely analysed data and information.

---

2 Ratcliffe (2016).

3 These academics are: Dr. Adrian James, Senior Lecturer and researcher at the University of Portsmouth's Institute of Criminal Justice Studies. Dr. Elke Devroe, Associate Professor and criminologist at the University of Leiden's Institute of Security and Global Affairs; and. Dr. Monica den Boer, Adjunct Professor in the Department of Security and Criminology at Macquarie University in Sydney, Australia and Director of SeQure Research and Consultancy.

Objective and added value

ILP is not a new subject within the OSCE. Some OSCE field operations are already engaged in supporting participating States in the implementation of ILP or some components of the model. Even though the partial or full implementation of ILP in countries within the OSCE region has yielded positive results, there seem to be discrepancies between the meaning of, the approach to, and ways of implementing ILP.

This guidebook aims at explaining and outlining the framework as well as the main components of ILP in order to enable a consistent understanding and implementation of ILP in the OSCE area. Its purpose is to serve as a practical tool for policy-makers, law enforcement decision-makers and criminal analysts in their efforts to improve the professionalism, effectiveness and efficiency of the police. The guidebook will provide a number of practical examples of good practices in implementing ILP, based on experience from OSCE participating States and international organizations, which can be tailored to national circumstances.

Although especially aimed for policy-makers, higher-level officials and law enforcement managers, this guidebook also serves all law enforcement and training institutions as well as universities and academia.

There is diverse academic and theoretical literature on ILP as well as a range of technical guidance material on single components of the ILP model, such as technical guidance handbooks from UNODC listed in the reference chapter, and national handbooks. This guidebook integrates some of this material, thus meeting the identified need for a guidebook on the general ILP approach, which can be used as a framework material for all OSCE participating States and Partners for Co-operation. It covers ILP in a comprehensive way, from the theoretical framework, through definitions and the introduction of key concepts and main components of the model, to a practical presentation of ILP implementation, including information analysis, threat assessments, decision-making and organizational structures.

In accordance with its comprehensive concept of security, the OSCE regards the protection of human rights, the rule of law, and democratic principles as an integral element of security. Participating States have recognized that security cannot be achieved at the expense of human rights, but that both are inclusive and mutually reinforcing objectives. Accordingly, law enforcement measures to address security threats can only be effective if they comply with human rights. Therefore, a separate chapter focuses on legal considerations, human rights and data protection to inform the discussion of the ILP concept and its practical implementation throughout this guidebook.

Structure of the guidebook

After briefly introducing the most common models of policing in Chapter 1, Chapters 2 and 3 focus on clarifying and presenting definitions of ILP and key terms within the concept. Chapter 4 gives a short overview of the main potential advantages in applying ILP to contemporary law enforcement. Chapter 5, drafted by the OSCE Office for Democratic Institutions and Human Rights (ODIHR), highlights human rights and data protection issues that apply to ILP. The criminal intelligence process, including analysis, is the backbone of ILP and the basis for the decision-making framework presented in the guidebook. Therefore, Chapter 6 explains the six traditional steps of the intelligence cycle and how it is applied within the ILP context.

Having covered the ILP conceptual model, human rights and data protection, and the criminal intelligence process, Chapter 7 focuses on the operationalization and practical implementation of ILP, starting with a graphical presentation of the proposed OSCE ILP model and a short description of each of its main components. This is followed by a sub-chapter where some challenges are identified and key implementation requirements are introduced. As analysis and assessment reports and other criminal intelligence products are the basis for strategic and operational planning, this guidebook repeatedly underlines the importance of the relationship between analysis and decision-making. Therefore, a separate sub-chapter covers decision-making within ILP, which is followed by sub-chapters 7.4 and 7.5 on local, regional and national criminal intelligence mechanisms and departments as well as proposed structures of tasking and decision-making meetings. These chapters provide clear suggestions on how to practically apply ILP at the national, regional and local levels from a law enforcement management point of view. Chapter 7 ends with a short overview of training essentials for all levels engaged in implementing ILP.

The last Chapter 8 of the guidebook introduces practical examples of ILP implementation, starting with ILP in addressing serious and organized crime, by presenting two commonly recognized threat assessment methodologies, the EU Serious and Organized Threat Assessment (SOCTA) and the Sleipnir threat and risk assessment tool. This is followed by the presentation of ILP in five countries: United Kingdom, Germany (North-Rhine Westphalia), Sweden, Republic of Serbia and Montenegro. In addition, the chapter examines how ILP can increase effectiveness and efficiency in two additional areas of law enforcement, namely community policing and counter-terrorism and VERLT.

1. Contemporary policing models

Researchers and the law enforcement literature commonly break law enforcement methodologies into five policing models; traditional policing, community-oriented policing, problem-oriented policing, computer statistics policing and ILP. Each of these models has different strategic goals, strengths and weaknesses, and can complement others when used concurrently. For example, ILP is increasingly being applied to reinforce community policing as it provides clear processes, communication procedures and management structures for data and information gathering, analysing and disseminating.[4] Another example is where the traditional, reactive model is the predominant one but ILP is only applied to countering serious and organized crime. A common factor of the first four above-mentioned models, and frequently presented as a weakness for contemporary law enforcement, is their focus on local areas and threats.

Rapid and significant changes on a global scale have changed the criminal environment as such these methodologies fail to possess the qualities required to address the more serious threat of transnational organized crime. As such, intelligence-led policing is the only method uniquely positioned to effectively combat transnational organized crime.[5]

Traditional policing is probably the best known of the policing models and is still the standard style of law enforcement. It refers to a reactive and incident-driven style in which police officers respond to crimes and requests for service or reactions. Answering calls, receiving complaints, randomly patrolling communities for a visible police presence and looking for crimes that have occurred or are occurring are the essence of traditional policing. Whereas the traditional policing model views reacting to issues of security and public safety as the task of the police, community policing focuses on the partnership between the police and the public in proactively addressing security and safety concerns.

4 See sub-chapter 8.3 on ILP and community policing.

5 Bell and Congram (2013: 19).

Community-oriented policing aims at building trust and increasing communication between the police and the public. Community policing programmes include creating community forums with the participation of representatives of various community groups and institutions where safety concerns, including local crime incidents and developments, are discussed and addressed.

In **problem-oriented policing**, the identification and analysis of "the problem" is the basic focus of police work, rather than a crime, a case, a call, or an incident. The model places emphasis on the problem behind crime or safety concerns. The police are to proactively build prevention strategies to try to solve problems, rather than just react to their harmful consequences.

Computer statistics model (CompStat) is a management system, originally modelled after "the broken windows theory", whereby minor crimes are addressed in order to reduce major crimes. Based on analysis of statistics of crimes already committed, individual local law enforcement commanders are responsible for carrying out local actions, which are designed accordingly.

2. Information, knowledge and intelligence

Before elaborating further on ILP, it is necessary to clarify a few key concepts. The word *intelligence* has a number of different definitions, depending on context, cultures, languages and traditions. In the literature reviewed for drafting this guidebook, the use of the word indicated that it simultaneously indicates a methodology, a structure, a process and a product. The review also showed conflicting views and an unclear understanding of the meaning of the concepts *data*, *information* and *knowledge*.

> "The lack of clarity and of a common understanding of criminal intelligence terminology and processes hampers information sharing between agencies."
>
> — **International Association of Chiefs of Police (2002)**

Hence, it is necessary to address and clarify the meaning of these concepts. After researching documents published by UNODC, UNDPKO, INTERPOL and the European Union (EU) as well as academic literature, this guidebook uses the following generally accepted definitions of the above concepts:[6]

Data are raw and uninterpreted observations and measurements. Examples include features of criminal activity that are easily quantified, such as crime reports and other crime statistics, databases of offenders and police tasks.

Information is data put in context and empowered with meaning, which gives it greater relevance and purpose.

Knowledge is information that has been given an interpretation and understanding. When a person has added his/her wisdom to information, it becomes knowledge.

Intelligence is data, information and knowledge that have been evaluated, analysed and presented in a decision-making format for action-oriented purposes.

---

6 Definitions of "data", "information", "knowledge" and "intelligence" are based on: Ratcliffe (2016: 70-74); UNODC, *Criminal Intelligence – Manual for Analysts* (Vienna: United Nations Publication), (2011a: 1); INTERPOL "Criminal Intelligence Analysis." *Fact Sheet* (2014); and Council of the European Union, "Council Framework Decision of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union." *Official Journal of the European Union* (2006/960/JHA, 18 December 2006).

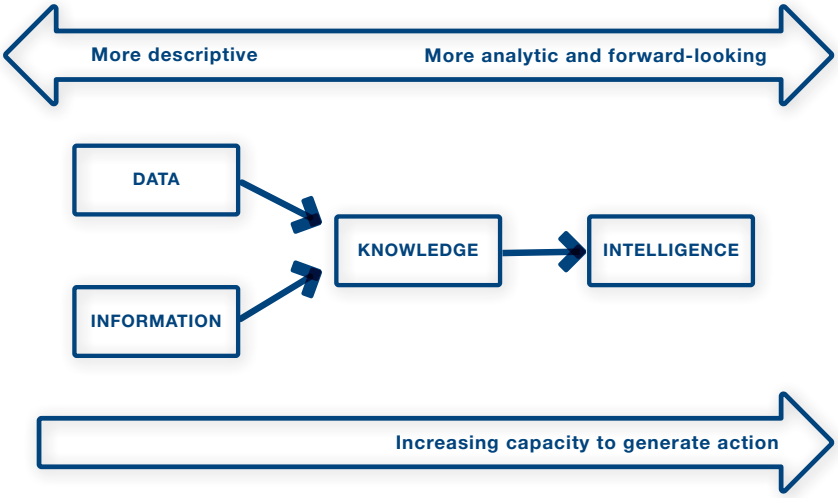


Figure 2.1 **From data to intelligence**

Source: Ratcliffe (2016: 72).

At a local police station, residential burglary incidents are inserted in the police database. These computer records are **data**. When a crime analyst accesses and maps the data, and recognizes an emerging pattern of new burglaries in an area, this becomes **information.** In essence, raw data have been enhanced with sufficient meaning to recognize a pattern. If the analyst subsequently discusses and shares this information with a detective, their understanding and insights become **knowledge.** After collecting further data and information, and analysing them, the detective and the analyst are able to build a picture in their minds, one that undoubtedly has gaps but that also has enough substance to support hypotheses and contain implications. The crime analyst and the detective draft an Operational Analysis Report and brief a senior officer. He/she decides to investigate and launch a surveillance operation to target burglars based on the **intelligence** from the analyst and the detective.

Note: A simplified and rephrased example from Ratcliffe (2016: 73-74).

3. Defining intelligence-led policing

As with the concepts addressed in Chapter 2, it emerges that there are various and even conflicting ideas on defining ILP. Some believe that ILP refers to conducting threat assessments, while others claim that it refers to the process of gathering data and information. These viewpoints provide valuable contributions to and components of the ILP framework, but do not cover the comprehensive concept of ILP. These diverse interpretations of ILP are understandable because it is relatively new[7] and is an evolving concept. Until recently, ILP was mainly used in connection with organized crime and serious offenders. Positive experience has convinced professionals and academics of a more inclusive ILP framework that incorporates all police activities, i.e. a process model with organizational infrastructure to support how policing in general is conducted. These developments have moved analysis closer to the centre of all areas of policing, further stressing the close co-operation between the analysts and the law enforcement decision-makers. This requires decision-makers to know the potential of analysis and how to make use of analysis results. Thus, proactive policing embedded in ILP calls for new skills and competencies of analysts, policymakers, law enforcement managers and other decision-makers. This important subject is addressed further in Chapter 7. Even though this guidebook encourages a pro-active application of ILP to all possible areas of policing, most countries already implementing ILP have limited its operational application to serious and organized crime, prolific offenders, criminal hotspots and crimes that generally cause public concern.

> "Intelligence-led policing emphasizes analysis and intelligence as pivotal to an objective, decision-making framework that prioritizes crime hotspots, repeat victims, prolific offenders and criminal groups. It facilitates crime and harm reduction, disruption and prevention through strategic and tactical management, deployment and enforcement."
>
> — **Ratcliffe (2016: 66).**

7 The UK Home Office first introduced the concept of intelligence-led policing in 1993 but it was first operationalized by the Kent Police. After 9/11, US law enforcement authorities adopted ILP as a methodology to counter terrorism. See further in Peterson (2005).

ILP refers to a management framework for criminal intelligence and planned operational police work, in which intelligence is the foundation for defining priorities, strategic and operational objectives in the prevention and suppression of crime and other security threats. It also includes making the appropriate decisions on operational police work and actions, the rational engagement of available human resources and allocation of material and technical resources.[8]

While ILP challenges the traditional and dominant reactive, response-based policing, its adoption and the alignment of law enforcement to proactive thinking, prioritization and planning will not change the fact that the police will always need to be reactive to security incidents and committed crimes. In an organizational structure where relevant information is systematically gathered, shared and analysed within a defined strategy, priorities and goals, ILP is designed to assist law enforcement managers to make informed and evidence-based decisions – not only in their strategic prioritization, but also in operational day-to-day planning. In this sense, ILP complements traditional, reactive policing.

ILP is a top-down, decision-making and a managerial model, although communication and information sharing within the model work both ways. Community policing is, in contrast, a typical bottom-up approach, aimed to enhance trust and confidence between police and the public.

> "Intelligence-led policing is crime fighting that is guided by effective intelligence gathering and analysis – and it has the potential to be the most important law enforcement innovation of the 21st century." – **Kelling and Bratton (2006: 5).**

8 Ministry of Interior of the Republic of Serbia, *Handbook on the police intelligence model* (2016: 16).

The 4-i model (*intent*, *interpret*, *influence* and *impact*) is helpful in explaining the roles and the relationship between key actors of the ILP concept: the criminal environment, the criminal intelligence analyst and the police decision-maker. All four "i" components must be in place and function properly if ILP is to work to its potential. The model places emphasis on the relationship between the criminal analysis and the decision-makers. The decision-makers (managers) task, direct, advise and guide the criminal intelligence analysts. First, the decision-makers have to ensure that their *intentions* are explained and understood. Second, the analysts *interpret* the criminal environment, and third, *influence* the decision-makers with the analysis findings. Based on these findings, the decision-makers (fourth) *impacts* on the criminal environment through strategic management, action plans, investigations and operations as presented in Figure 3.1.[9]

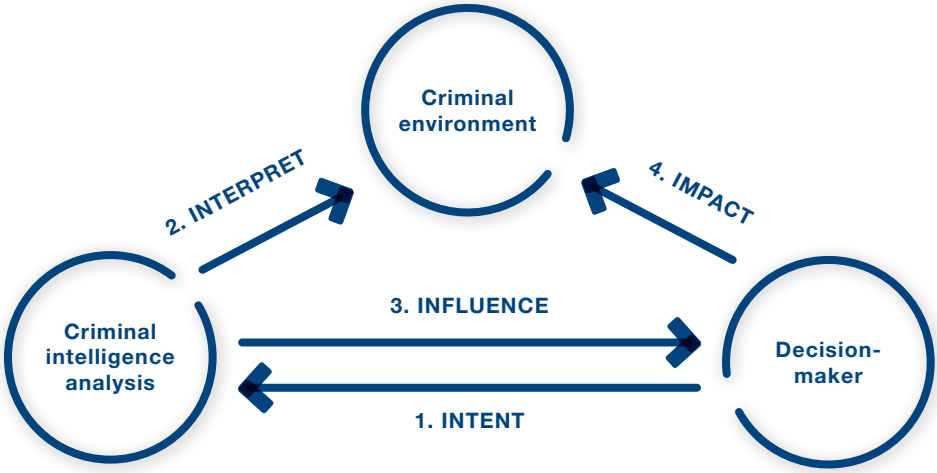


Figure 3.1 **The 4-i model: *intent, interpret, influence and impact***

Source: Ratcliffe (2016: 83).

9 In its technical guidance material, UNODC has underlined the central role of the analyst and analysis products in the decision-making process. See the tasking model presented in UNODC (2011b: 5).

4. The advantages of intelligence-led policing

In private industry and the business community, information and intelligence are key factors in creating competitive advantage. In this regard, law enforcement is no different since strategic advantage based on information, knowledge and intelligence increases the effectiveness of law enforcement to prevent crime and security incidents, and disrupt criminal groups and networks. But possessing information, knowledge and intelligence is not enough. An appropriate framework or a model is needed to manage the intelligence and to make maximum use of it, and to ensure that data and intelligence are gathered, processed and used in strict compliance with national laws and international human rights standards.

ILP allows for a forward-looking and pro-active approach to police management. Its successful application in recent years in a number of countries around the world to address serious crime and transnational threats has encouraged the development of the ILP concept from being mainly applied to countering organized crime to a more general strategic business model to address a wide variety of policing problems at the local, regional and national levels. This development is directly related to the search for law enforcement methods that would allow the police to have a greater impact on crime, crime developments and the social harm of criminality with limited resources and at times of increased demand for accountability.

In recent years, demand for police services and response have outpaced the resource availability of the police, raising the claim for prioritization and increased efficiency of law enforcement resources. At the same time, political and public expectations of accountability have been heightened. ILP has been presented as an option to address this, since it offers the rationale and the tools to analyse and assess threats to the public, allowing for more documented, transparent and accountable decision-making procedures to direct existing resources where they are most needed.

> "The need to introduce intelligence-led policing (ILP) should not be questioned. In times of budgetary and resource restrictions, each responsible individual and organization has to identify priorities to tackle major problems. To assist in prioritization, decisions have to be made based on facts and intelligence, the basis of all of which is information. ILP will contribute to optimizing the allocation of resources and concentrate efforts in a more structured manner. This helps to cope with increased sophistication and operational agility of criminals to subvert law and order."
>
> — **European External Action Service (2013: 12).**

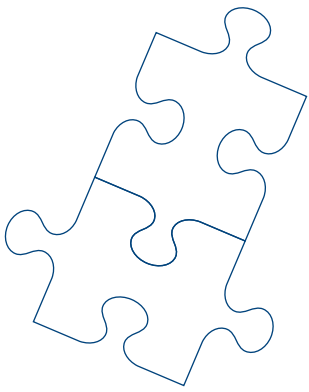
The fact that violent extremists related to recent terrorist incidents, including lone wolves, remained under the law enforcement radar has called for a proactive approach and highlighted the need for a comprehensive sharing and centralized analysis of relevant data and information. The realization that a terrorist attack and early detection of other serious incidents cannot be dealt with in a reactive way put ILP into the spotlight at the international law enforcement stage. This was apparent after the 9/11 attacks, reflected in the findings of the U.S. 9/11 Commission that concluded that there were various pieces of information held at different levels before the attacks, but due to the agencies' failure to share them, they could not be co-ordinated to provide a comprehensive picture.

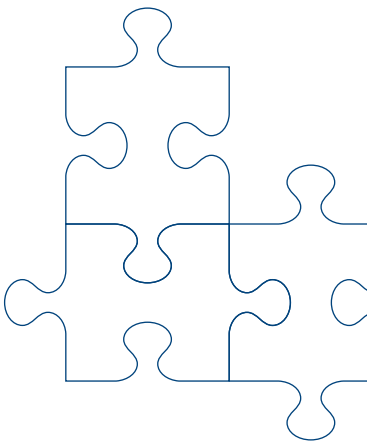
Risk identification and management is an integral part of modern policing. A properly functioning ILP approach to data and information gathering and analysis allows for identifying and assessing risks, including for major events, geographic areas, types of crime, social harm, serious criminals and criminal networks.

> "Studies suggest that while, in general, increasing numbers of police officers can be effective, it is more useful to consider how officers are deployed. Random patrol is not an effective tactic to reduce crime, but more focused tactics that are drawn from an evidence base (a fundamental component of intelligence-led policing) can have crime prevention benefits beyond the amount of time officers spend at a crime hotspot."
>
> — **Ratcliffe (2016: 139).**

The ILP model incorporates clear organizational and management structures including decision-making and tasking mechanisms at the local, regional and national levels, as well as defined co-operation and communication processes between domestic law enforcement authorities and within international co-operation.

Improved data and information management is an important advantage of ILP for contemporary law enforcement. In the modern era of information flow, the ILP model provides for directed and targeted collection of relevant data and information, in line with a defined policy, strategy, objectives and priorities.





5. Legal considerations, human rights and data protection

Human rights compliance is important for both the short- and long-term effectiveness of policing, including ILP. Law enforcement actions that fail to respect and protect human rights are counter-productive in the long term because they undermine public trust in the police and are also ineffective. Ethnic profiling,[10] for example, is discriminatory, and it has also proven to be ineffective because it can be easily circumvented. Criminal groups can avoid detection by recruiting people who do not conform to the pre-determined profiles. Alternative, legitimate profiling techniques based on specific evidence about criminal behaviour and intelligence rather than discriminatory assumptions can be used as a more effective policing tool.

ILP within the human rights framework

Human rights norms are set out in international legal instruments and standards such as binding treaties like the International Covenant on Civil and Political Rights (ICCPR) and the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).[11] To give effect to the rights set forth in these treaties, States must put in place a legal and institutional framework for the realization of human rights at the domestic level. Within this framework, it is among the main duties of the police to protect individuals from acts that compromise their human rights, including those resulting from crime and terrorism, and to respect these rights. In combating and preventing crime, the police must operate in accordance with domestic law and international standards. As a proactive form of policing, ILP must also be firmly grounded in the human rights framework. It should increase the protection of the individuals' rights and freedoms, and must be carried out in a manner that fully respects human rights, which is in line with key principles of democratic policing.[12]

---

10 Ethnic profiling in policing means exercising police powers against individuals based on stereotypical, broad and unqualified assumptions related to nationality, ethnicity or religion.

11 All OSCE participating States, except the Holy See, have ratified the ICCPR and are therefore parties to the treaty. Furthermore, 47 OSCE participating States are also members of the Council of Europe and thus are also parties to the ECHR. OSCE participating States have pledged to fulfil their obligations arising from the international human rights treaties to which they are parties in conformity with international law. See Conference on Security and Co-operation in Europe, *Final Act* (1975).

12 OSCE (2008b).

General human rights principles

In order to ensure that ILP activities comply with international human rights standards and do not have a detrimental impact on the enjoyment of human rights, a number of fundamental principles must be met in devising and implementing ILP at the national level:

The legal, administrative and institutional framework for the implementation of ILP: First, ILP must be based on clear and precise legal and administrative provisions, which set out the conditions in which it is to be implemented and provide for adequate safeguards to ensure that it does not compromise human rights. The domestic ILP framework must include laws and regulations that clearly and precisely define the powers granted to relevant agencies and the requirements that need to be met in the collection, processing, analysis and sharing of different types of information and intelligence. All domestic laws, regulations, policies and practices concerning ILP must be in full conformity with international human rights standards and OSCE commitments. Furthermore, law enforcement officers involved in ILP must be adequately trained to apply these laws and regulations in conformity with international human rights standards.

Legality, necessity and proportionality of limitations of human rights: While a number of human rights, such as the prohibition of torture and certain elements of the right to a fair trial, are absolute and cannot be restricted under any circumstances, international human rights treaties allow for the imposition of limitations on certain rights, but only within strictly defined parameters.[13] Accordingly, interferences imposed in connection with ILP are permissible only if they are prescribed by law, necessary in a democratic society in the interest of a legitimate aim specifically referred to in relevant international human rights standards, and proportionate towards this aim: i.e. the right is the rule, the limitation must remain the exception, and the interference must always represent the least intrusive means to achieve the aim.

Equality and non-discrimination: In accordance with their international human rights obligations, OSCE participating States have committed to ensure human rights and fundamental freedoms to everyone within their jurisdiction, without distinction of any kind such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.[14] Upholding equality before the law and prohibiting discrimination are essential duties of the police in a democratic society.[15] In collecting, processing and analysing information and intelligence, law enforcement must therefore, for example, refrain from discriminatory profiling. Similarly, as regards decision-making based on intelligence, authorities must be alert to avoid over-policing of particular communities, which may amount to discrimination. Particular attention should also be paid to the differential impact that strategic decisions in policing may have on women and men. A diversity and gender-sensitive approach should therefore be mainstreamed into all ILP activities, which

13 Rights that may be subject to limitations include the freedom of movement, the right to privacy, freedom of expression, assembly and association and the freedom to manifest one's religion or beliefs.

14 OSCE (1989), *Concluding Document of the Vienna Meeting 1986 of Representatives of the Participating States of the Conference on Security and Co-operation in Europe, held on the basis of the provisions of the Final Act relating to the follow-up to the Conference.*

15 OSCE (2008b).

should be regularly reviewed for any discriminatory impact they may have on women and men, or on particular communities.

Effective remedies, oversight and accountability: International human rights standards provide for the right of everyone whose rights or freedoms are violated to an effective remedy and to have a claim for such a remedy determined by a competent judicial, administrative or legislative authority.[16] Since ILP may lead to potentially far-reaching interferences in a broad range of human rights, effective and accessible remedies for human rights violations that may result from ILP are essential. Furthermore, solid internal and external oversight mechanisms need to be in place in order to ensure accountability of institutions and individual law enforcement officers involved in ILP. Such mechanisms may include control and supervision of the executive, legislative oversight committees and independent external oversight and complaints mechanisms that give individuals avenues for redress. Judicial control over activities such as covert intelligence gathering is particularly important to provide appropriate safeguards against abuse in the application of ILP.

The right to privacy

Collection of data and information, but also its processing, analysis and sharing, which are all integral elements of ILP, may have serious implications on the protection of human rights, in particular but not only, the right to privacy.

Article 17 of the ICCPR stipulates that no one shall be subjected to arbitrary or unlawful interference with one's privacy, family, home or correspondence, and that everyone shall have the right to the protection of the law against such interference.[17] For interferences not to be "arbitrary" or "unlawful", a number of requirements, similar to those referred to above, have to be met: they have to be prescribed by law, which in turn must comply with the provisions, aims and objectives of the ICCPR; and they must be reasonable in the particular circumstances.[18] OSCE participating States reconfirmed the right to the protection of private and family life, domicile, correspondence and electronic communications, and the need to avoid improper or arbitrary intrusion by the State in the realm of the individual.[19]

Different overt and covert methods of gathering information present various degrees of interference with the right to privacy. Some of these methods, such as the use of special investigation techniques and other covert investigation measures, including surveillance on private premises or in homes, interception of communications, the use of undercover agents and informants as well as accessing bank accounts and other confidential information, are explored in further detail in the OSCE, ODIHR/TNTD manual, *Human Rights in Counter-Terrorism*

16 United Nations General Assembly, "International Covenant on Civil and Political Rights (ICCPR)." *No. 14668, United Nations Treaty Series, Vol. 999* (New York: 16 December 1966): Art. 2(3).

17 A similar provision on the right to respect for private and family life is contained in Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)* (4 November 1950): Art. 8.

18 United Nations Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* (8 April 1988).

19 OSCE, *Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE* (Moscow, 3 October 1991).

Investigations.[20] Effective control by judicial or other independent authorities through prior authorization, supervision or ex post facto review is paramount for such measures to be lawful. Furthermore, they should be used only in serious cases and in a way that is proportionate to the seriousness of the matter that is being investigated.[21]

An issue that has received considerable attention is the consequences of mass surveillance of communications on the right to privacy. The European Court of Human Rights found surveillance systems to be in violation of the right to privacy, which allow for the interception of communications and masses of data of virtually anyone in a country, even persons outside the original range of an operation, and where the ordering of such measures is taking place entirely within the realm of the executive and without an assessment of strict necessity.[22] As opposed to targeted surveillance, which is commonly based on a prior suspicion and subject to prior judicial or executive authorization, mass surveillance programmes do not allow for an individualized case-by-case assessment of the proportionality prior to such measures being employed and therefore appear to undermine the very essence of the right to privacy.[23]

Data protection

Data protection is an important part of the right to private life of particular relevance to ILP. The United Nations Human Rights Committee, the body tasked to monitor implementation of the ICCPR, has stressed that the gathering and holding of personal information on computers, data banks and other devices must be regulated by law. Furthermore, effective measures have to be taken to ensure that information concerning a person's private life does not reach the hands of anyone who is not authorized by law to receive, process and use it.[24] A number of international and regional instruments contain more specific data protection principles that need to be respected with a view to ensuring full compliance with the right to privacy.

---

20 OSCE, ODIHR/TNTD (2013: 33-46). On legal as well as technical aspects of electronic surveillance in particular, see also UNODC, *Current practices in electronic surveillance in the investigation of serious and organized crime* (2009).

21 OSCE, ODIHR/TNTD (2013).

22 European Court of Human Rights. *Case of Szabo and Vissy v. Hungary.* Application no. 37138/14 (Strasbourg: 12 January 2016); and European Court of Human Rights. *Case of Roman Zakharov v. Russia.* Application no. 47143/06 (Strasbourg: 4 December 2015).

23 United Nations General Assembly. "Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson." Annual Report to the UN General Assembly, 23 September 2014, A/69/397: para 52. For more information on mass digital surveillance for counter-terrorism purposes, see United Nations General Assembly. "Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism." Report to the UN Human Rights Council, 21 February 2017, A/HRC/34/61: 10-13.

24 UN Human Rights Committee (April 1988).

The *Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* for example, requires parties to the Convention to ensure that personal data undergoing automatic processing are:

- obtained and processed fairly and lawfully;
- stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are stored;
- accurate and, where necessary, kept up to date;
- preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which these data are stored.[25]

Furthermore, the Convention prohibits automatic processing of sensitive data, such as data revealing racial origin, political opinions, religious or other beliefs as well as data concerning health, sexual life or criminal convictions, without appropriate safeguards in domestic law.[26] It also provides for safeguards and remedies that should be available to persons who are the subjects of the data that are being stored.[27]

The Convention sets strict limits on restrictions to these provisions similar to those referred to above. Any restrictions must be provided for by law and must be necessary in a democratic society in the interest of a legitimate aim enunciated in the Convention, such as state security, public safety, or the suppression of crime.[28] "Necessity", as understood in international human rights standards, comprises proportionality towards the aim pursued.

The OSCE, ODIHR/TNTD manual, *Human Rights in Counter Terrorism Investigations*, provides an overview of international best practices based on the above principles and other international standards in this area.[29] These should also guide policy-makers and law enforcement officers in devising and implementing ILP in order to ensure compliance with international human rights standards.

---

25 Council of Europe. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series, No. 108 (Strasbourg: 28 January 1981): Art 5. All 47 member States of the Council of Europe, and therefore also a large majority of OSCE participating States, are parties to the Convention.

26 ibid. Art. 6.

27 ibid. Art. 8.

28 ibid. Art. 9.

29 OSCE, ODIHR/TNTD (2013): 30-31. Other relevant instruments include, for instance, United Nations General Assembly, Resolution 45/95, "Guidelines for the regulation of computerized personal data files." A/RES/45/95, 14 December 1990.

Other potential human rights risks related to intelligence-led policing

Privacy rights, including data protection, are instrumental for the exercise of a broad range of other rights and fundamental freedoms, such as: the right to freedom of opinion and expression; freedom to seek, receive and impart information; freedom of peaceful assembly and of association; and freedom of religion or belief, among others. But the gathering and use of information and intelligence may also directly affect the enjoyment of other rights such as the right to a fair trial, the right to liberty and security of person, and the prohibition of torture and other ill-treatment.

For example, in policing public protests, the use of crowd management strategies known as "kettling" for intelligence gathering purposes by compelling peaceful protestors and even bystanders to disclose their names and addresses as they leave the "kettle" has been criticized for the chilling effect it may have on the exercise of the right to peaceful assembly.[30] An arrest based on the registration of the person concerned in a law enforcement surveillance database that does not afford adequate protection against arbitrary interferences with the right to privacy and not based on other information that demonstrates a reasonable suspicion that the arrested individual has committed or was about to commit a concrete offence, is contrary to the right to liberty and security.[31]

Concerning the collection, processing, analysis and sharing of information, including as part of ILP, it is also of particular importance that the use of torture-tainted information in judicial proceedings is absolutely prohibited under international law. Its admission as evidence in court violates the rights of due process and a fair trial.[32] But even when not intended to be used in judicial proceedings, the collection, sharing and receiving of torture-tainted information shall be prohibited.[33]

These concerns are particularly relevant where information and intelligence are shared across borders. The use of torture-tainted information from a third country, even if the information is obtained only for operational purposes, can make the receiving State complicit in the commission of internationally wrongful acts.[34] Hence, in the implementation of ILP, appropriate safeguards should be in place to ensure that information and intelligence obtained by unlawful means, whether within or outside of the country, are not used in contravention with international and domestic law.

---

30 United Nations General Assembly. "Special Rapporteur on the rights to freedom of peaceful assembly and of association Maina Kiai, Addendum, Mission to the United Kingdom of Great Britain and Northern Ireland." Report to the UN Human Rights Council, 17 June 2013, A/HRC/23/39/Add.1: para 38.

31 European Court of Human Rights. *Case of Shimovolos v. Russia.* Application no. 30194/09 (Strasbourg: 21 June 2011).

32 See United Nations General Assembly. "Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, Juan E. Méndez." Report to the UN Human Rights Council, 10 April 2014, A/HRC/25/60: para 21.

33 ibid.: para 73. See also OSCE and TNTD/ODIHR (2013: 28).

34 ibid. See also United Nations General Assembly. "Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin." Report to the UN Human Rights Council, 4 February 2009, A/HRC/10/3: paras 55-57; and OSCE, ODIHR/TNTD (2013: 28-29).

6. The criminal intelligence process

The intelligence process, traditionally called the *intelligence cycle*, describes and outlines six widely recognized standard steps used to transform raw data and information into value-added intelligence aimed for action. The process ideally starts with a decision or a tasking, followed by a planning stage, after which analysts engage in collecting information and data that must be evaluated according to a formally recognized evaluation system (see page 35). The next step is the actual processing stage, starting with collating and structuring available data and information, and inserting them into a database. The data and information are then analysed, which results in the production of an intelligence product to be disseminated to the client (manager, investigator or others that task the analysts or request their analysis support) and other relevant stakeholders. The intelligence product is evaluated by the client with reference to their needs and demands. The received feedback is used to improve the current product or as methodological input for future similar products.

The intelligence cycle is not a static sequence of six steps, but rather a dynamic process, where different phases are closely interlinked and feed into one another, making it necessary for analysts to go back and forth within the intelligence cycle. The cycle outlined in Figure 6.1 provides a structure and a process that is ordered and easy to understand, and can be used as the basic process both for strategic and operational analysis.[35]

35 UNODC has published a number of technical guidelines on criminal intelligence and the intelligence process for front-line police officers, intelligence officers, analysts and law enforcement managers. See www.unodc.org.

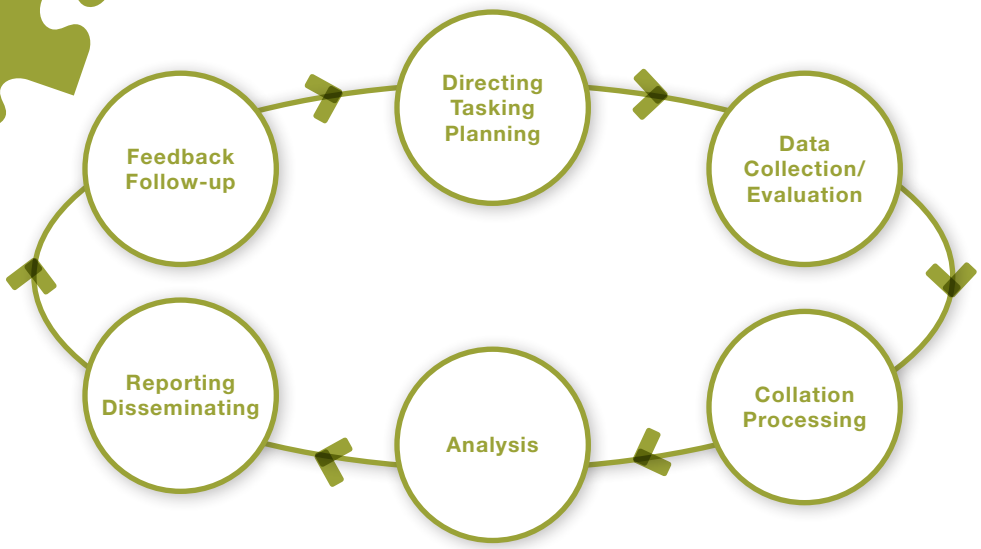


Figure 6.1 **The criminal intelligence cycle**

The intelligence cycle is initiated by a clear tasking for the sake of developing concrete intelligence products. The criminal intelligence process, however, is conducted on several different levels and is often not limited to the intelligence cycle. In addition to the cycle highlighted in Figure 6.1, there might be a need for a wider and more constant process of strategically assessing intelligence requirements. This ongoing assessment identifies extant and emerging threats and intelligence gaps, and is carried out in accordance with strategic priorities, policies and goals. This process requires a well-functioning and structured intelligence organization and Standard Operating Procedures (SOPs) that enable the intelligence cycle to be fed with information and that define expected result of the cycle and its follow-up. The strategic assessment of intelligence requirements as well as the criminal intelligence cycle feed into the strategic planning process of a country, reflecting national, regional and local strategic priorities. This is further explained in the next chapter.

The following sub-chapters will explain the main components and purpose of each step within the intelligence cycle.

6.1 Tasking and planning

The intelligence cycle is initiated by a management decision, tasking analysts to develop intelligence on the problem or topic of inquiry. Based on this tasking, management and the analyst will negotiate and agree on the Terms of Reference (TOR), a document laying down the scope, main objectives, content and timeline of the intelligence product. The TOR is the official starting point of the intelligence cycle.

The importance of a clear tasking and agreeing on the objectives of an intelligence product is often underestimated. In order to task the analysts clearly, law enforcement managers and decision-makers must know the potentials and limitations of intelligence analysis. Similarly, analysts have to know how to assist investigators, managers and decision-makers (clients) by creating tailored products and targeted recommendations. The tasking phase, at times called the "decision phase", requires close co-operation between the analysts and the clients. They need to agree on the *subject of inquiry, objectives, aim, scope, timeline* and *form of reporting, including the dissemination and recipient of the intelligence product*. The analyst needs to be clear on the expectations and the intent of the client.

It is essential to treat such tasks as projects and carefully plan their different steps. Complex projects may require a considerable amount of time and significant resources. Based on the TOR and relevant to the scope of the project, the analyst should develop a detailed project plan comprising the agreed objectives, scope and timeline, as well as the sequence of activities, and list of the resources necessary to successfully complete the task. This phase is indispensable for it will serve to guide the collection and subsequent analysis of information. It is therefore important that the project plan be endorsed by management. The project plan should also take into consideration possible legal and data protection issues that may arise in the implementation of the intelligence project. In particular, if the use of personal data or covert methods of gathering data and information are involved, the legal requirements and possible restrictions should be taken into consideration at an early stage in the planning process to ensure that the collection, sharing and use of data and information are carried out in strict compliance with national laws and international standards.

Clear planning saves time in the long term and allows for the efficient use of resources, resulting in an increased output quality.[36] It also reduces the risk that the collection, storing, sharing and handling of data and information are not in line with national and international legal standards, and thereby jeopardizes the success of the entire project. With an appropriate tasking and planning, the products of intelligence analysis can assist in developing strategic plans to tackle current problems and prepare for anticipated ones.[37]

The strategic assessment and the intelligence requirement

Intelligence requirements have their roots in the strategic assessment process. The assessment provides law enforcement executives with an overview of the policing problems that the institution faces or may face. Prepared by the intelligence unit/department/agency, it is a wide-ranging document reflecting national, regional and local strategic priorities. The preparation of the document is the first stage in the strategic planning process.

36 See further in sub-chapters 6.2 and 8.1.

37 UNODC (2011b: 10-13).

All extant and emerging threats identified during the scanning process of the strategic assessment should be addressed in the document. Nothing meaningful should be omitted. The document is then considered in a strategic forum where these threats are considered in the context of the resources available. Priorities are matched to resources. The number of threats included in any control strategy is determined by the resources available to address them; those afforded the highest priority by the strategic forum are included in a control strategy. This sets the operational agenda, which in turn is overseen by middle managers who accept personal responsibility for each of the identified priorities and undertake to formulate plans to manage these threats.

The control strategy is likely to contain a mix of national, regional and local priorities so that it might include otherwise seemingly unconnected phenomena such as international terrorism, street robbery and drunken driving. It should remain unchanged until the next strategic assessment is prepared or until more significant threats are identified and brought to the attention of the executive. In the interim, operational/tactical assessments presented at regular operational/tactical meetings ensure that these priorities remain the focus of the institution. Operational/tactical meetings review the operational plans established by middle managers and provide a forum for new threats to be discussed. This ensures that managers remain focused on threats identified for action by their executives.

Other threats identified in the strategic assessment are not to be ignored even if there are insufficient resources to deal with them immediately; they are added to the control strategy to create the intelligence requirement. It is the responsibility of all law enforcement staff members in an institution to prioritize their work in accordance with the control strategy. It is the duty of the secretariat or intelligence department to keep the intelligence requirement under review, assessing whether previously identified threats deserve greater attention (perhaps as emendations to, or as additions to a new control strategy) and continuously scanning for any new threats that may emerge.

6.2 Collection and evaluation

Collecting information for intelligence projects is a challenging process. While analysts must ensure the collection of sufficient data to cover all aspects of the topic(s) to be analysed, they must avoid data overload and the collection of unnecessary or inadequate information. Key to this phase is the intelligence staff's knowledge of the existence, relevance, accessibility and reliability of all sources and agencies that are selected for a particular collection task, as well as knowledge of any legal limitations and authorization requirements that apply to the use of different types of information sources. Knowledge of and access to internal and external data and information sources, and awareness of potential limitations and requirements are prerequisites for effective collection and intelligence analysis.

Examples of data and information sources used by criminal analysts:

Official sources:

- Ministries, state agencies, prosecution
- Law enforcement databases
- International organizations
- Financial intelligence units
- Neighbourhood officers
- Border control data
- Public records
- Patrol officers
- Investigations
- Surveillance
- Informants

Non-official sources:

- Non-governmental organizations
- Transportation industry
- Anonymous reports
- Commercial sector
- Financial sector
- Civil society
- Social media
- Community
- Academia
- Media

The collection plan

The development of a collection plan is the next step to follow the agreement on the TOR and the project plan, as described above. The collection plan is imperative for ensuring the orderly and precise collection of relevant data and information to meet requested/tasked requirements. This has to be seen as a continuous process that is able to adapt and respond to changes of requirements. The collection plan is based on the definition, objective, scope and timeline of the task, and describes: **what** information must be collected or is available, including the goal and value of the data collected; **which** sources should be used; **where** the information can be obtained; **how** the information can be obtained and **who** must collect it; **how** much data can be handled; and **when** each piece of information should be collected. In some instances, it may be necessary to include **why** certain data and information need to be collected. As the overall project plan, the collection plan also needs to take into account different legal requirements that will apply to the collection tasks depending on the type of information to be collected as well as the sources and means used to obtain it. [38]

Developing a detailed collection plan, which includes a needs assessment and the necessary legal authorizations as well as the supervision requirements that may apply, is essential to the success of the project. The plan will therefore ensure that all parties involved follow the agreed objectives and applicable standards.

Evaluation

Simultaneously with or immediately after the collection of information, the data need to be evaluated within the context in which they had been acquired. Data evaluation needs to be based on objective professional judgment, since the quality of data determines the validity of

38 See OSCE, ODIHR/TNTD (2013: 34).

the developed intelligence. The evaluation considers the validity and reliability of information and its usefulness to the task.[39] A common first step is to identify what is important and what is irrelevant, as well as assess the urgency to act on the information. The reliability of the source and the validity and accuracy of the information need to be separately assessed by the officer/analyst who obtained and registered that particular information.[40]

All sources and all information should be evaluated according to a formally recognized evaluation system. The 4x4 or 5x5x5 are the two most widely used systems.[41]

Table 6.1 **Evaluation codes according to the 4x4 evaluation system**

EVALUATION OF SOURCE		EVALUATION OF INFORMATION	
A	Completely reliable in all instances	1	Accuracy not in doubt
B	Usually reliable	2	Known personally to the source but not known personally to official passing it on
C	Not usually reliable	3	Not known personally to the source but corroborated by other available information
D	Reliability cannot be assessed	4	Accuracy cannot be assessed or corroborated in any way (at this time)

Table 6.2 **Evaluation codes according to the 5x5x5 evaluation system**

EVALUATION OF SOURCE		EVALUATION OF INFORMATION	
A	Always reliable	1	Known to be true without reservation
B	Mostly reliable	2	Known personally to the source but not to the person reporting
C	Sometimes reliable	3	Not known personally to the source but corroborated
D	Unreliable	4	Cannot be judged
E	Untested source	5	Suspected to be false

Note: The 5x5x5 system includes "Handling Codes", which are not explained here.

Evaluation of the relevance, reliability and accuracy of information as well as the determination of a handling code for its further use are essential for the accuracy of the final intelligence products and the modalities of their dissemination. But the evaluation is also important from

39 National Policing Improvement Agency, *Practice Advice on Analysis* (Association of Chief Police Officers, 2008).

40 UNODC (2011b: 25-28).

41 ibid. See also information on the 6x6 evaluation systems. The 5x5x5 system includes "Handling Codes", which are not explained here.

a human rights and data protection perspective. As set out in Chapter 5, data protection standards require, among other things, that recorded personal information is accurate, adequate, relevant and not excessive in relation to the purpose for which it is being stored. The evaluation is therefore key to demonstrate that recording of information, which represents an interference with the right to privacy of the data/information subject, is justified, necessary and proportionate, and therefore permissible under applicable human rights and data protection standards.

Evaluators should also be conscious of other possible human rights issues that may be relevant to how certain information may be used. This is particularly important when evaluating information from third countries if there are grounds to believe that the information may have been obtained by unlawful means. The use of evidence obtained by torture and other ill-treatment in judicial proceedings, for example, is absolutely prohibited under international law. But even when not intended to be used in court proceedings, information or intelligence obtained by such means should also be disregarded.[42]

6.3 Collation and processing

The processing and collation phase requires an adequate and consistent system. This phase entails sorting, prioritizing and referencing the collected information. During the collation phase, the analyst organizes and structures gathered information, converting it to an indexed and cross-referenced format, and transfers it into a storage system (i.e. database). Verifying the relevance, accuracy and usefulness of information is an important step before inserting it into a storage system. It is vital to have an accessible system established from which information can be retrieved and analysed.

The processing of information can be so closely interlinked with the analytical phase, making a clear separation difficult.[43]

6.4 Analysis

As with different types of intelligence, there are diverse expressions of analysis classifications. Operational analysis in one organization is called tactical analysis in another, and network analysis in one police department is called link analysis or link-charting in the neighbouring country. The most common analysis classifications are strategic analysis, operational analysis and tactical analysis. This guidebook groups tactical and operational analysis together under operational analysis.[44]

42 OSCE TNTD/ODIHR (2013: 28).

43 National Policing Improvement Agency (2008).

44 UNODC, INTERPOL and Europol use this same classification. See UNODC (2011b: 35-38).

Strategic analysis supports decision-making, policy-making, planning and prioritization; allocation of police resources; and determines the appropriate approach for addressing crime types. It also provides intelligence-led support to front-line law enforcement by facilitating the identification of key threats, vulnerabilities, risks and opportunities for action (threat and risk assessments). Strategic analysis does not include personal information.

Operational analysis assists in the management and front-line enforcement of shorter-term tasks to achieve operational objectives, and supports ongoing investigations. Operational analysis can include personal information on suspects.

The analytical process is needed to transform raw data and information into actual intelligence and to direct both short-term operational and long-term strategic law enforcement goals. The credibility and scope of the analysis greatly depend on the quality and accuracy of the previously gathered data on the one hand, and the skills of analysts on the other hand. Throughout the analysis of information, as well as all other phases of the intelligence cycle, close co-operation between the analysts and the clients (officers, investigators, managers), including the organization of regular review meetings, is absolutely crucial to ensure that intelligence is developed in line with intelligence needs and/or customer requirements.

The analysis phase is central to the intelligence process because it concerns the identification and examination of the meaning, context and essential features of available information. The analysis of data draws attention to information gaps, the strengths and the weaknesses of data, and defines the way forward. The main goal of the analysis phase is to derive meaning from the original information in order to enable intelligence to be put to practical use. When results of criminal intelligence analysis are directly linked and respond to the tasking/problem of inquiry, the analysis becomes valuable as an operational tool.

The analytical process consists of two phases: *data integration* and *data interpretation*. The first phase (data integration) combines evaluated and collated information from different sources in order to develop initial hypothesis and predictions, identify a pattern of intelligence and draw inferences. The second phase (data interpretation) entails going beyond the data available and interpreting it. In this phase, the initial hypotheses are tested, resulting in supporting, modifying or refuting previously developed hypotheses.

A *hypothesis* is a tentative working theory that is based on previously developed indicators and premises drawn from available data and information and that requires additional information in order to corroborate or contradict previous assumptions. Hypotheses help to identify intelligence gaps, to focus further data collection, and to reach accurate inferences, conclusions, predictions and estimations.

Developing and testing hypotheses has increased in its importance within intelligence analysis. Hypotheses contain a great deal of speculation and therefore need to be tested

(confirmed, modified or rejected) by analysts. The testing of hypotheses should include: the hypothesis' pro and contra arguments, its implications, a review of the thinking process, and collection and revision of the needed data. A hypothesis or any inference should contain answers to the following key questions (often referred to as the "5Ws' and 1H"):

- Who? Key individual/individuals
- What? Criminal activities
- How? Methods used
- Where? Geographical information and scope
- Why? Motive
- When? Timeframe

Using hypotheses to test and explore a criminal phenomenon or a safety concern is an important step in strategic thinking, moving from "tell me everything you know" to a specific and action-oriented process. This technique and the others introduced in this chapter underline that the training, skill level and experience of both decision-makers and analysts are vital for successful ILP.

Examples of analytical methods

The National Intelligence Model (NIM) of the United Nations Office on Drugs and Crime (UNODC) derives from nine analytical techniques and products, which corroborate informed strategic and/or operational decision-making and the development of professional knowledge in effective proactive law enforcement techniques:

- ***Crime pattern analysis*** is a broad term of a range of analysis types, including trend identification and hotspot analysis.
- ***Demographic/social trend analysis*** assesses the impact of socio-economic and demographic changes on criminality, as well as population shifts and homelessness.
- ***Network analysis*** assesses the direction, frequency and strength of links between collaborators in a criminal network.
- ***Market profiles*** assess the criminal market for a particular commodity, such as drugs or prostitution.
- ***Criminal business profile*** determine the business model and techniques employed by offenders or organized crime groups.
- ***Risk analysis*** assesses the scale of risks or threats posed by offenders or organizations to individual potential victims, police and the public.

- ***Target profile analysis*** describes the criminal, his/her strengths and weaknesses, the lifestyle, networks, criminal activities and potential interdiction points in the life of a targeted offender.

- ***Operational intelligence assessment*** evaluates if collection of information follows the previously agreed objectives and identifies gaps in the operation's intelligence efforts (used in large-scale projects and operations).

- ***Results analysis*** evaluates the effectiveness of law enforcement activities and monitors the progress of plans.

Source: Based on UNODC (2011b: 35-38).

In addition to the above-mentioned analysis methods, analysts use a number of other qualitative analysis techniques,[45] all of which share a common purpose: they are tools to break down complex problems into more manageable analytical portions.

6.5 Reporting and dissemination of intelligence products

Intelligence products are the output of the intelligence process and are generally disseminated in the form of clearly structured and concise reports. Intelligence analysis reports aim at reflecting objective and accurate information, and identifying and recommending effective strategic or operational interventions. To ensure the practical value of the intelligence products, they should always be clear and concise. As highlighted earlier, a close collaboration between the analyst and the client, including the organization of regular review sessions, is therefore inevitable for delivering a targeted intelligence product and introducing its findings. A good general approach when drafting any kind of intelligence products is the *inverted pyramid writing*, starting by addressing the most important messages to the client and then moving to more general issues.

Depending on the need of the customers, these products can be divided into strategic and operational intelligence products.

The aim of **operational analysis reports** is to support ongoing investigations and short-term operational and tactical tasks. Aimed at practitioners, such products must be concise, favour clear and direct wording, and focus on information with operational added value. Key findings must be listed at the beginning, allowing the reader to quickly grasp the main information and decide how to prioritize the information received. Intelligence products should then

45 For descriptions and examples of these techniques, see UNODC (2011a). See also the Problem-Oriented Policing website: www.popcenter.org/about/?p=whatiscpop. In addition, reference is made to information and guidance on a number of analysis types and methods on the website of the International Association of Law Enforcement Intelligence Analysts: www.ialeia.org

go into more detail, starting with brief descriptions of the operational background, followed by their aims and objectives. The core of intelligence products should provide detailed information on the case, explain the analysis process leading to the hypothesis and clarify the findings. The products should conclude with intelligence requirements and recommendations for actions. Operational intelligence products are an important source of information for strategic products.

The aim of **strategic analysis reports** is to support informed decision-making and the design of operations. Various types of documents can be prepared, depending on requirements and objectives:[46]

Early warning notifications/intelligence notifications highlight new or recent changes, trends and developments in the environment, which can be thematic or geographical. The primary purpose is to describe the changes and assess possible effects on criminal markets, the security situation, and the community or a wider geographical area. Such notifications are short and specific, aiming to proactively and rapidly inform the client of a new change or a trend, and give a brief indication on expected effects of this change or trend.

Threat assessments analyse and evaluate the threat of criminal phenomena. They can focus on organized crime groups, specific crime areas or regions. The assessments usually have a medium- to long-term scope and are future-oriented. They provide decision-makers with strategic intelligence and recommendations.

Risk assessment reports describe the evaluation of potential risks, where the assessment of likelihood, impact and related vulnerabilities is added to the threat assessment. A classic example is a risk assessment report presented in preparation for a major event.

Situation reports are mainly descriptive. Their objective is to provide a detailed overview of a topic. Contrary to threat assessments, they generally do not include recommendations for actions and are limited to factual findings. They can focus on a variety of topics, from a specific crime area or modus operandi, to a specific criminal group or geographic area.

The last step in the intelligence process is the dissemination of the intelligence product and briefing the customer(s) of its content. Consumers of intelligence analysis can be investigators, prosecutors, law enforcement management and other police or government agencies. When possible and appropriate, the intelligence product should be shared with the public. This can be beneficial for law enforcement by raising public awareness on specific topics (as part of crime prevention), increasing transparency and visibility, and receiving valuable information from the public in response to published reports. It is important to choose the right method/format for disseminating and presenting the intelligence product to targeted audiences and to ensure that it arrives in a timely manner in order to support decisions and ac-

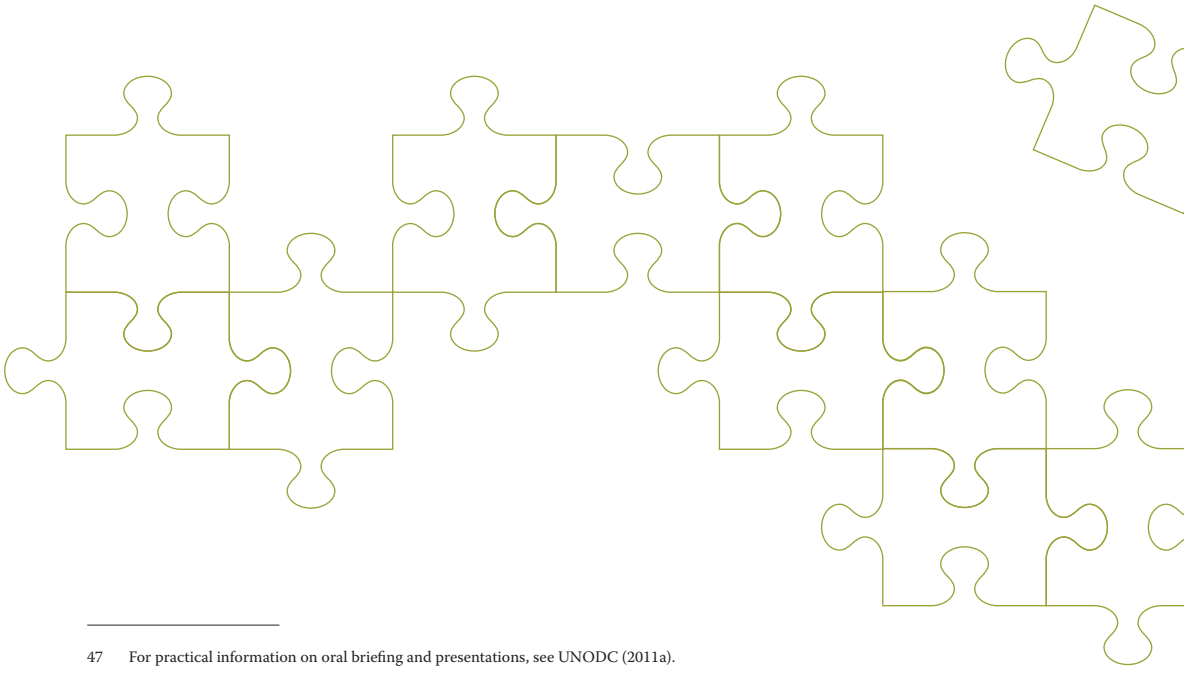
46 In its Factsheet on Criminal Intelligence Analysis, INTERPOL classifies analytical products into analytical reports, threat assessments for regions or specific crimes, risk assessments for a particular event, and intelligence publications (bulletins, monthly reports, etc.). Europol classifies analysis reports first into operational and strategic reports, but divides strategic reports into threat assessments, situational reports and intelligence notifications.

tions.[47] The dissemination phase is critical to the whole structure of the ILP model since it informs the customer as well as all appropriate police entities about relevant criminal activities, phenomena and perpetrators. Due to the sensitivity of data usually presented in intelligence products, a clear and transparent regulation has to be adopted, based on the basic principles of "right to know" and "need to know" in accordance with national and international human rights and data protection standards.

Further details on the dissemination of intelligence products need to be spelled out in respective national handbooks or manuals, in line with national instructions and legal requirements, and in accordance with international human rights standards.

6.6 Feedback and follow-up

The importance of an active collaboration between the client/decision-maker and the analyst is repeatedly highlighted in this guidebook. This also applies to the evaluation of the intelligence product and the feedback from the client, the decision-maker or other users of the analytical product. The analysts and their managers must know if the product has met requirements and if recommendations contributed to decisions or follow-up actions. The analysts must also receive feedback on potential improvements. Sending a feedback form to the client soon after submitting the analysis report and presenting the intelligence product is a very useful practice. A follow-up meeting should be organized where the intelligence product, the feedback, the co-operation and subsequent decisions, actions or operations are discussed. Such arrangements not only increase the quality of the task in question, but are also necessary for professional development.



47 For practical information on oral briefing and presentations, see UNODC (2011a).

7. Implementing ILP

This chapter will introduce a graphical presentation of a recommended OSCE ILP model and explain its main components, followed by a closer examination of key requirements in operationalizing and implementing ILP. Although it is tempting to present a matrix or a form for implementing ILP, there is neither a universal template nor should there be one, because local and national circumstances vary considerably. Each country must assess its status and develop its own implementation plan in the light of the existing legal framework, culture, needs, resources, and other basic national/local factors, and tailor its approach to these key requirements. Nevertheless, based on some commonly accepted principles, the OSCE has developed a framework model for ILP implementation, which OSCE participating States are invited to make use of when adopting and implementing ILP.

Although national circumstances vary, research has shown that achievements of national ILP policies, strategies and implementation generally depend on the following key success factors:

- a clear legislative framework for ILP, which is in conformity with international human rights and data protection standards, and includes clearly defined powers and processes for agencies to collect, analyse and share relevant intelligence;
- organizational structures that facilitate clear strategic direction and operational co-operation as well as decision-making processes in a multi-agency environment and appropriate oversight;
- technology to facilitate information sharing through interoperability of systems;
- knowledge and skills of all relevant staff; and

- a collaborative culture of intelligence sharing to support decision-making across operating domains.[48]

All these issues will be addressed later in this guidebook.

7.1 The OSCE ILP model

As explained in Chapter 3, ILP is a top-down managerial and decision-making framework. It provides a structure, methodology and multiple processes for a systematic gathering, sharing and analysis of relevant information, which serves as basis for informed planning and decision-making in law enforcement management. ILP has been called a law enforcement business model, i.e. a methodology guiding the conduct and management of policing.

The 4-i conceptual model presented in Chapter 3 highlights the relationship between the three key actors within ILP: the criminal environment, the criminal intelligence analysts and the decision-makers. The 4-i model shows that the decision-makers task and direct the analysts by explaining their *intentions*. The analysts *interpret* the criminal environment through their analysis and *influence* the decision-makers with the findings. Based on the analysis products, the decision-makers *impact* the criminal environment through law enforcement actions.

> "Intelligence-led policing is a business model for policing […] able to incorporate areas of policing activity that are not related to crime per se but are still significant problems for communities and police agencies. With this evolution, intelligence-led policing is moving to becoming the 'all-crimes, all hazards, all-harms' business approach that is sought by many in policing." **– Ratcliffe (2016: 67).**

Figure 7.1 is a simplified graphical presentation of the main steps, the key actors, procedures and products in putting the ILP concept into practice. The model can be applied partly or in full at the national, regional or local law enforcement levels.[49]

48 See Australian Criminal Intelligence Management Strategy 2012-2015 (Commonwealth of Australia, 2012); and James et al. (2016).

49 This graphical illustration of the proposed OSCE ILP model is developed by the Strategic Police Matters Unit of the OSCE Transnational Threats Department, based on Ratcliffe's (2016) definitions. The presentation of Information Flow in UNODC's *Police Information and Intelligence Systems* (2006) was also used in the development of the chart.

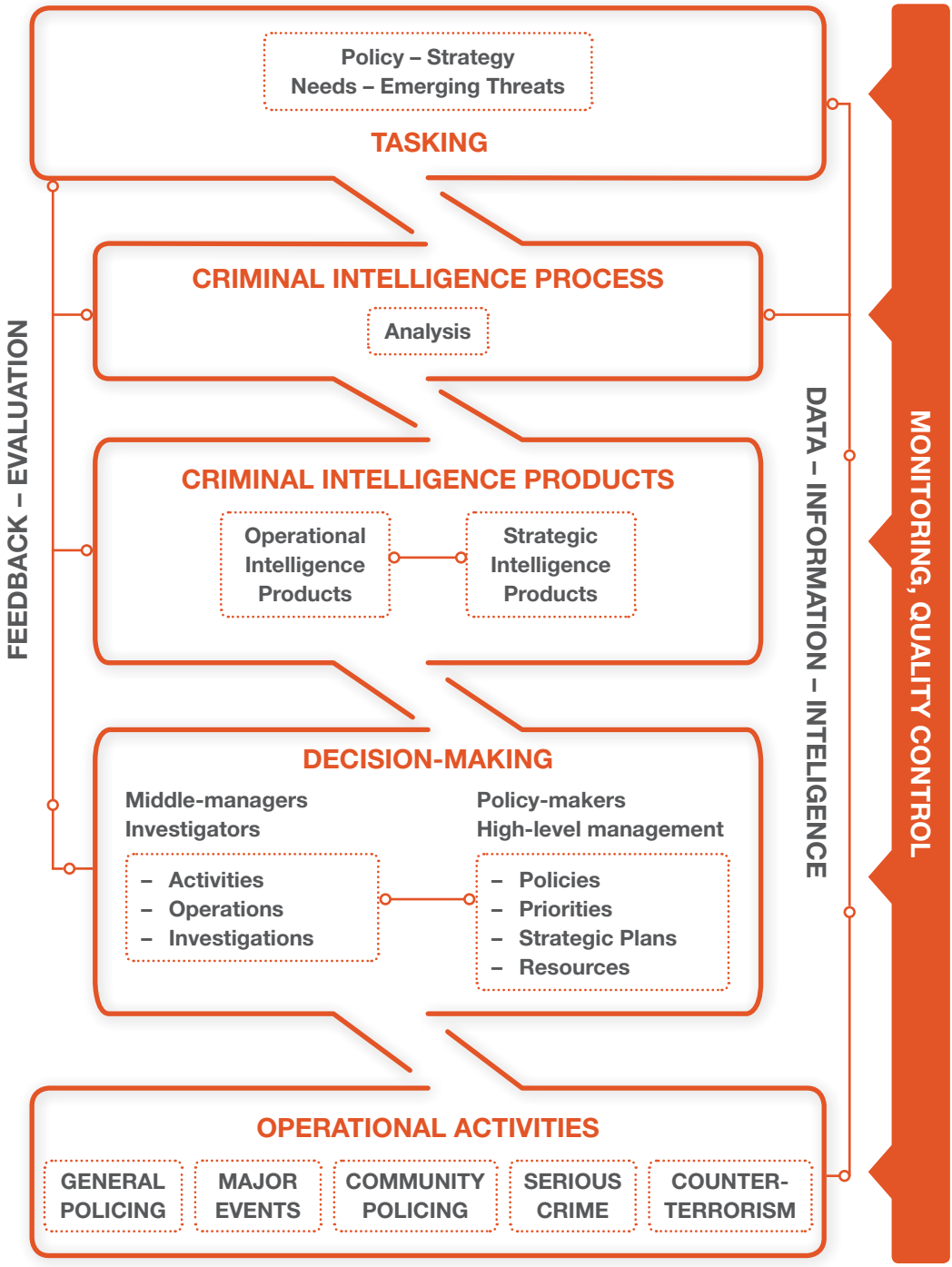


Figure 7.1 **The OSCE intelligence-led policing model**

The ILP model includes the following main steps and components:

TASKING

Based on policy, strategic and operational plans, emerging threats or identified needs, the national, regional or local law enforcement management tasks and provides directions to the analysis management, which distributes tasks to individual analysis departments, units or individual analysts.

ANALYSIS WITHIN THE CRIMINAL INTELLIGENCE PROCESS

Following directions and tasking from management or requests from investigators, analysts develop intelligence in line with a defined intelligence process. While the analysis constitutes the processes' core component, the process furthermore includes the collection, processing and collation of information. (A detailed description of the six steps of the criminal intelligence process is given in Chapter 6.)

CRIMINAL INTELLIGENCE PRODUCTS

The analysis process generates strategic and operational criminal intelligence products, which are used as a basis for developing strategic and operational plans, and for supporting criminal investigations and other law enforcement operations as well as for prioritizing and allocating human and technical resources.

DECISION-MAKING

This guidebook recommends that each country maintain an ILP decision-making structure at the national, regional and local levels, where analysis reports/intelligence products are used as a basis for decisions. A suggestive mechanism is described in sub-chapter 7.5, and examples of national good practices are presented in sub-chapter 8.2.

OPERATIONAL ACTIVITIES

Figure 7.1 lists five examples of policing areas where the principles of ILP can be applied. This is by no means an exhaustive list, and pro-active law enforcement, based on evaluated and analysed data and information, can be applied to many other areas of policing. The operational policing areas generate data, information and intelligence that are forwarded through clearly defined communication channels and stored in databases that allow for further analysis.

Data and information flow

For ILP to be well functioning, all law enforcement officers need to share and forward, through clearly defined mechanisms and communication channels, relevant data, information and intelligence they receive and gather throughout their activities and daily work. Sharing of data, information and intelligence should be an obligation of all law enforcement officers defined in domestic law or other formal instructions.

Feedback and evaluation

Analysts and analysis managers receive feedback on the quality of their analysis and criminal intelligence products from law enforcement managers, investigators and other users of their reports. The main quality indicators of the criminal intelligence products are their conformity with defined methodologies and standards, and the extent to which they meet the expectations and requirements of their users, especially with regard to strategic and operational decision-making.

Monitoring and quality control

Creating and maintaining a system of monitoring and quality control of the ILP model is the responsibility of the high-level law enforcement management. This applies to all plans, objectives, processes and steps, including evaluation of criminal intelligence products, follow-up of tasking and decisions, adherence to human rights and data protection standards, and resources allocated to tasks. Each country should set up its own quality management and quality control system. In addition to internal monitoring and quality control, ILP-related functions such as the collection, storing, processing and sharing of data, information and intelligence also need to be subject to independent oversight.[50]

Although the ILP model is broken down into five main steps and sub-processes, it has to be underlined that all the components of the model are interactive and feed into one another, making it often necessary for previous steps to be revisited. For example, the analysis process frequently reveals intelligence gaps, which at times call for a new tasking or an investigation.

As mentioned above and frequently highlighted in this guidebook, all law enforcement personnel are active participants in and providers to ILP. The ILP model relies on data and information from all levels, departments and units of the law enforcement. Therefore, awareness and training as well as clear ILP SOP for all levels need to be in place as well as appropriate safeguards, accountability and oversight mechanisms.

7.2 Challenges and key implementation requirements

Research has identified several challenges and preconditions for ILP to work to its potential. It has been revealed that ILP can have a meaningful and measurable impact only if it is conducted by substantial organizational, cultural and leadership change.[51] It has also been noted that reluctance to make such reforms have proved a significant obstacle to the implementation of ILP. Still adding to the challenges, adopting and implementing implementing ILP often "threatens the established order, the culture, the identity of the organization and the norms,

50 For an example of a good practice, see Ministry of Interior of the Republic of Serbia (2016: 45-49).

51 Flood and Gaspar (2009).

values and morale of its staff" and "staff rarely welcome change".[52] The predominance of performance culture and operational statistics, where emphasis is placed on measuring results, has been highlighted as one important reason for the reluctance for change within law enforcement.[53] Thus, introducing ILP as a new law enforcement decision-making framework poses a particular challenge because it often requires new management methods and a cultural change within the police leadership. To maximize the potential of ILP, a comprehensive change management including thorough preparation, consultation and awareness measures must take place throughout all levels of the organization before and during implementation.

> "Ultimately, the prospects for any organizational reform invariably are limited by the extent to which those with real power in the institution believe change is both in their best interests and will deliver practical benefits for the institution."
>
> **– James (2016: 26).**

In addition to the above challenges, other identified prerequisites for a successful ILP implementation include:

- quality staff selection, adequate training and skilled staff;
- competent direction, management and control of the intelligence work;
- suitable databases, IT equipment and analysis software; and
- qualified managers who know how to make use of intelligence analysis products.[54]

The following points provide general guidance for planning the adoption and implementation of ILP. Even though the basic ILP model can be applied everywhere, these points should be put into the national and local context.[55]

National legal framework allowing for implementing ILP, in line with international legal standards

- National legislation should include specific provisions on ILP and allows for its implementation.
- Gathering, storing, processing and sharing of data and information must be based on national law, which strictly complies with international human rights and data protection standards. OSCE participating States are encouraged to request technical assistance and advice to assess the compliance of those laws with international standards.

52 James (2017: 7).

53 Parliamentary Joint Committee on Law Enforcement, *Inquiry into the gathering and use of criminal intelligence* (Canberra: Parliamentary Joint Committee on Law Enforcement, Commonwealth of Australia), (2013: 47-49).

54 James et al. (2016: 24-25); Ratcliffe (2016: 127).

55 This guidebook will not give a detailed list due to diverse country specifics, but rather, will focus on general and common issues throughout the OSCE participating States, based on reviewed literature and collected inputs from nominated law enforcement experts who reviewed and gave inputs to the guidebook drafts.

- The ILP framework, methodologies and internal processes, and the sharing and use of criminal intelligence products should adhere to OSCE principles of democratic policing, which reaffirm the importance of the rule of law, human rights, data protection, police ethics, accountability and transparency, and external monitoring and control.[56]

Political support and high-level governmental and managerial commitment

- Political support, high-level governmental/ministerial and law enforcement leadership-level awareness and commitment must be secured and clear before adopting or implementing ILP.
- The full potential of ILP will not be reached unless all levels of the law enforcement know the model, its structures and processes as well as their roles and responsibilities within it.

Organizational-wide approach

- ILP can be applied to all areas of policing.
- ILP should be applied throughout the organization, not only in specialized units.
- Efforts to change the culture towards one that underlines the "need to share" information should be an integral part of the change management in introducing and implementing ILP.
- ILP has analysts working in direct support of decision-makers at all levels of the organization.

National strategic law enforcement planning, based on strategic analysis, including threat assessments

- National strategic plans, including prioritization, should be formulated and based on strategic analysis and assessments.
- These plans should be further developed into operational action plans.
- Human, technical and financial resources should be allocated in accordance with these plans.

Strategic and operational tasking meetings

- Both operational and strategic tasking meetings should take place regularly at the local, regional and national levels (see further sub-chapter 7.5).
- Effective criminal intelligence gathering and analysis has proved to generate more investigative and operational opportunities than law enforcement can possibly meet. Therefore, identification and careful tasking and prioritization must be an integral task of the strategic and operational meetings.
- To secure intelligence-led decision-making, operational and strategic intelligence products should be integrated in the decision-making and tasking frameworks.

Gathering and sharing of data, information and intelligence

- All law enforcement officers should be obliged by law or other formal decisions to share information they have received regarding a suspected crime or suspected criminals through mechanisms and communication channels that are clearly defined and in accordance with domestic law and international standards.

---

56 OSCE (2008a: 12-13).

- Sufficient safeguards must be in place to protect the human rights of people mentioned in information that has been gathered for analysis purposes.
- Necessary arrangements must be in place to protect identities and security of informants and security of whistle-blowers.
- Within applicable domestic and international legal frameworks, handling codes and data protection law, authorities should allow sharing of data and information between state agencies and other official institutions.
- The relevant authorities may make formal arrangements that allow for obtaining and using relevant data and information from sources that are external to state agencies, including local authorities, non-governmental organizations, civil society, private industry, regional and international organizations, the media and the public on the condition that these arrangements are within the limits of applicable domestic and international legal frameworks. These arrangements must also provide for the appropriate safeguards to ensure that the authorities do not obtain access to such data contrary to human rights and data protection standards.
- National information evaluation systems, including handling and dissemination codes, should be decided and introduced in a formal decision.
- All law enforcement officers should be well familiar with these codes and apply them to all information they receive and submit.

Centralized criminal intelligence agency/department

- This guidebook recommends that each country operates one centralized national criminal intelligence department (NCID).
- The NCID should be staffed by members of various agencies.[57]
- Representatives of different law enforcement entities and other authorities represented in the NCID should have access to their agency's data and information, and should be allowed by law to share them with representatives from other entities/authorities represented within the NCID, pertinent to domestic and international legal frameworks.
- The NCID should be responsible for a national criminal intelligence database.
- The NCID should be responsible for carrying out strategic and operational analysis, including threat assessments, at the national level.
- The NCID should assist regional/local criminal intelligence analysis departments/units when relevant.[58]

Criminal analysis and threat assessments

- National authorities should present formal decisions and SOPs on transparent analysis and threat assessment methods and processes.
- Types and structures of criminal intelligence products should be decided at the national level, providing all the law enforcement with a common reporting framework.
- Criminal intelligence reports based on commonly accepted international standards and formats, clarify and inspire cross-border and international co-operation in criminal matters.

---

57 See further in sub-chapter 7.4.3 on central-level criminal intelligence mechanism. See also an example of a good practice from Sweden in sub-chapter 8.2.3.

58 Recommendations on managing intelligence units are presented in UNODC (2011b: 51-59).

IT interoperability and security

- Interconnected, interoperable or single-platform IT structures supporting ILP should be operated at the national, regional and local levels.
- NCID should have access to all available data, information and intelligence held by regional and local criminal intelligence departments and other law enforcement bodies.
- Appropriate security features according to formal decisions and SOP, national legislation and international standards need to be in place, including detailed logging and internal control mechanisms, as well as clearly defined and registered access levels.
- These formal decisions and SOP should cover physical security, document security, IT security and personnel security, including vetting and background checks of staff where relevant.[59]
- Criminal intelligence databases and sharing of data, information and intelligence should be subject to monitoring and control of an independent external control authority established by law to ensure compliance with national legislation in line with international human right standards and data protection provisions, and provide for effective and accessible remedies in case of violations.

Feedback mechanisms and practice

- Managers and analysts receiving information from law enforcement officers should give feedback to encourage further sharing.
- Managers, investigators and other users of analysis products should give feedback to the analysts on the quality of the analytical products to stimulate progress and improvements.

Quality management and control

- The national law enforcement management is responsible for: developments and maintenance of a system of monitoring and quality control on all levels of the ILP implementation; tasking and decision-making; objectives and outcomes; internal processes; criminal intelligence products; material and equipment; and human resources including training and staff performance.
- The complete intelligence process in each country should be subject to internal and external oversight mechanisms.

Co-operation and intelligence-sharing with the law enforcement community at the regional and international levels

- In line with domestic legislation, international standards and mutual legal assistance instruments, national strategic analysis and threat assessments should be shared with relevant co-operation countries and with applicable regional and international organizations.

59 UNODC (2011b: 39-50).

- Intelligence-sharing with authorities of a foreign state should be based on national law that outlines clear parameters for intelligence exchange, including the conditions that must be met for information to be shared, the entities with which intelligence may be shared, and the safeguards that apply to exchanges of intelligence.[60]
- Pro-active steps should be taken to establish joint intelligence-led investigations and operations at the regional and international levels, based on common criminal challenges identified and presented in analysis and threat assessment reports.

7.3 Analysis and decision-making in law enforcement

Pro-active law enforcement requires intelligence and strategic planning. Adding to increased requirements for enhanced resource efficiency, transparency and accountability, a number of external and personal influence factors affect decision-makers, as presented in Figure 7.2.

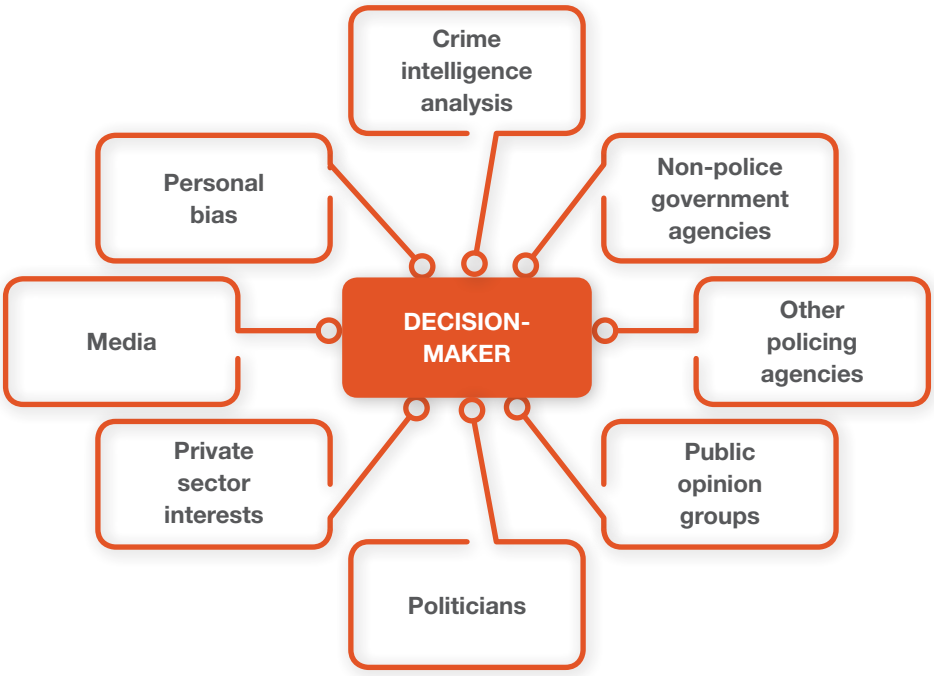


Figure 7.2 **External and personal influences on decision-makers**

Source: Ratcliffe (2016: 118).

60 United Nations General Assembly. "Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin." UN Human Rights Council, 17 May 2010, A/HRC/14/46: Articles 26, 38 and 90.

Decision-makers in modern law enforcement have to live with the fact that a wide range of influence factors affect their everyday work and their key decisions. Quality police management, including decision-making, requires quality analysis products and skilled analysts who are able to support managers with providing tailored reports. Since most law enforcement decisions directly affect peoples' lives, and since all law enforcement officers are accountable for their actions,[61] the information basis for their decisions becomes especially important. These facts still emphasize the relevance of ILP as a managerial decision-making framework.

> "It is often emblematic of weak police decision-making systems that analysts task themselves or take the lead in determining strategic priorities. Police leaders in mature decision-making systems take a more direct role in conveying their intent by tasking the intelligence and analysis unit. While remaining open to being influenced about emerging threats that might not be on their radar, experienced commanders do not leave the analysis arm of the police department foundering without guidance, but rather provide supervision and direction."**– Ratcliffe (2016: 83).**

Even though analysts must always build their analytical findings on neutral evaluation and assessment, they should have insight into the decision-maker's environment, including potential legal, political, organizational and financial constraints. This must be taken into account when developing and presenting recommendations. It is futile for the analysts to present recommendations that are clearly unfit for the clients or out of their reach.

7.4 Levels of criminal intelligence mechanisms

ILP requires organizational structures, administrative and decision-making procedures and communication mechanisms between all levels. This sub-chapter will present intelligence mechanisms (units/departments/agencies) that support the execution of ILP. One of the key tasks of each level's criminal intelligence mechanism is to provide management structures with analysis and assessment for making informed decisions.

61 Council of Europe, *The European Code of Police Ethics* (Strasbourg: Council of Europe Publishing, March 2002): Art. 26, 38 and 90.

7.4.1 Local/station-level criminal intelligence mechanism

The local-/station-level intelligence mechanism covers crimes, criminals, and security and safety problems affecting the basic police command unit at the community or police station level. Depending on size and structure, each local level should have a criminal intelligence unit or a team responsible for all relevant operational criminal intelligence tasks on its level. This unit should be headed by a commander of the same rank as heads of operational and investigations units at the local-/station-level.

Local-/station-level criminal intelligence supports local planning, operations and investigations. More specifically, it:

- supports general operational police services in addressing everyday crime and to maintain public security and order at the local or station level;
- provides analytical support to local-/station-level investigations;
- provides police registries, databases and criminal intelligence processes with data and information;
- submits relevant data, information and intelligence to regional and/or national criminal intelligence departments for further processing;
- conducts and presents analysis and risk assessments for local events; and
- provides analytical support to local crime prevention.

7.4.2 Regional-level criminal intelligence mechanism

The regional criminal intelligence section covers law enforcement tasks affecting more than one basic police command unit. Its key tasks and responsibilities are the identification of common regional criminal threats, the exchange of appropriate information, and provision of capabilities and resources to support local- and regional-level activities. The regional criminal intelligence section should be at the same level and headed by the same rank as heads of regional operations and investigations, directly under the regional police director.

The regional criminal intelligence department/section supports local criminal intelligence units upon request. Its main role is to support regional-level planning, operations and investigations. More specifically, it:

- develops and implements annual regional criminal intelligence plans;
- systematically collects relevant data, information and intelligence at the regional level and submits them to a regional centralized database, accessible to the centralized criminal intelligence entity in each country (henceforth the National Criminal Intelligence Department);
- forwards relevant data, information and intelligence reports to the local and national levels;
- conducts strategic analysis and assessments to support management decision-making and planning at the regional level;
- provides support to regional crime prevention; and
- supports investigations and operations against regional and cross-border crime, including transnational organized crime;

7.4.3 Central-level criminal intelligence mechanism

The NCID should be positioned within the national law enforcement headquarters (police directorate/national crime agency) and headed by a senior chief officer.

NCID's main role is to develop intelligence reports to support decision-making in countering serious national threats, in particular transnational organized crime, terrorism and VERLT. Key responsibilities include:

- developing and implementing an annual national criminal intelligence plan;
- drafting and presenting a national serious and organized crime threat assessment;
- drafting and presenting other strategic assessment to support national-level law enforcement management and planning;
- providing criminal intelligence support to the regional level;
- setting standards and co-ordinating criminal intelligence work within the country;
- acting as the national point of contact to foreign law enforcement authorities and organizations with regard to criminal intelligence work; and
- conducting research and striving for professional development at the local, regional and national levels.[62]

Ideally, the NCID should be a multi-agency law enforcement entity, staffed with experts from diverse relevant agencies and state institutions, each expert having access to his/her institution's information and databases, and allowed by law to share data and information with staff from other agencies/institutions represented in the NCID. Depending on security sector structures in each country, the following state authorities could be represented within the NCID:

- Border police
- Correction authorities
- Customs
- Financial Intelligence Unit (FIU)
- Coast guard/maritime police
- Intelligence and security agencies
- Police
- Tax authorities
- Specialized law enforcement agencies where relevant

Agencies/institutions represented within the NCID might prefer to draft formal co-operation agreements between themselves and the NCID. Within such agreements, some OSCE participating States have chosen to place representatives of the above agencies/institutions as liaison officers within the NCID.

62 See also recommendations for managing and setting standards for criminal intelligence units in UNODC (2011b: 51, 61).

7.5 Tasking and co-ordination meetings

A number of OSCE participating States have developed pro-active and intelligence-led decision-making mechanisms, commonly named "tasking and co-ordination meetings", "leading and co-ordination meetings" or "sharing and briefing meetings". *Tasking and co-ordination meetings* take place at all three levels: local, regional and national. Their main purpose is to: bring together relevant law enforcement representatives at each level to make decisions on plans, prioritization, operations and investigations, based on analysis and assessment documents; identify information/intelligence gaps to address; and decide on financial and human resource allocation. This set-up is at the heart of ILP as it moves analysis results into the management procedures, making the decision-making more informed, intelligence-led, transparent and accountable. Furthermore, creating criminal intelligence mechanisms that serve decision-making at each level allows the police management to prioritize law enforcement tasks in line with identified and assessed threats, and to allocate available financial, human and other resources to that prioritization. Identifying intelligence gaps, intelligence requirements and tasking analysis departments/units to meet these requirements is also an important task of the decision-making meetings at each level. To secure information flow and co-ordination between levels, the chair or another representative from the next level below participates in meetings above.

This guidebook suggests that tasking and co-ordination meetings be divided into *strategic tasking and co-ordination meetings* and *operational tasking and co-ordination meetings*.

7.5.1 Strategic tasking and co-ordination meetings

As the name indicates, these meetings should focus on strategic issues and are held much less frequently than the operational ones, typically twice a year or every three months. In some countries, *strategic tasking and co-ordination meetings* are held at all three levels, but more commonly, only at the central/national level. These meetings should focus on strategic planning and setting strategic priorities and objectives, based on strategic analysis and threat assessments as well as the organizational business planning and budget cycles. It is recommended that the *strategic tasking and co-ordination meetings* determine and set priorities for national intelligence requirements, prevention and enforcement, based on strategic analysis findings and threat assessments. Having made these sets of decisions, these meetings should decide on resources needed to implement the strategic choices.[63]

7.5.2 Operational tasking and co-ordination meetings

This guidebook recommends that operational ILP decision-making mechanisms be held at all three levels once a week or every two weeks. Operational and investigative managers should attend them together with managers from the criminal intelligence department and relevant analysis unit/department as well as other experts if required. It is recommended that the highest ranking operational manager head each meeting. Depending on levels and national/

63 See national examples of good practice introduced in sub-chapter 8.2.

regional/local circumstances, *operational tasking and co-ordination meetings* are mainly responsible for: converting strategic plans into action plans, matching requirements, priorities and resources; evaluating new or updated operational intelligence reports and making decisions on new investigations or operational activities, or to close or combine activities; identifying information and intelligence gaps and tasking criminal intelligence units/departments to fill them; and monitoring ongoing operational progress.

7.6 Training and awareness

Training is a key factor for progress in any organization. When planning and implementing ILP, it is essential to develop a training plan and conduct a co-ordinated training of all law enforcement. All staff members are expected to learn not only the skills necessary for their performance, but also understand the roles of other members in order to contribute to the overall ILP results. Through training, staff should understand ILP, the way the intelligence process works, what and how to contribute to the process, and how to make use of it. The culture of information sharing should be a special focus within training for all levels. In addition, training should include legal requirements related to ILP functions and relevant international human rights and data protection standards to an appropriate extent in accordance with the level and functions of the officials.

> "If intelligence-led policing is to succeed and develop as the central paradigm of policing in the twenty-first century, then addressing training and education in crime reduction practice for not only analysts but also police commanders and key decision-makers in the criminal justice system is going to be crucial and may very well be the key determinant in deciding the future of intelligence-led policing."
>
> **– Ratcliffe (2016: 143).**

High-level awareness

As earlier underlined, political support and high-level governmental commitment to ILP are prerequisites for successful implementation. This requires awareness-raising at higher levels, including among politicians, governmental officials in all relevant ministries and state agencies, prosecutors general and other key prosecution representatives, and high-level management of all law enforcement agencies and services.

Training of law enforcement leadership and management

The main goal of this training is to demonstrate how the ILP framework and analysis in particular can support policy-makers and law enforcement leaders in their decision-making and planning. A successful training of the leadership will result in an increased level

of understanding of the potential of ILP, how to task analysts, and how to make use of analysis products in operational and strategic decision-making and planning. Such training should also provide decision-makers with an understanding of relevant national and international human rights and data protection standards as well as possible human rights issues that may arise in ILP and how they can be addressed.

Training of analysts

This training is commonly divided into strategic and operational analysis training, in line with the two main categories of analysis. Analysts must undergo the most complex training in order to understand the role and functions of crime analysis within law enforcement and the legislative framework and legal requirements that apply to different methods of information gathering as well as sharing and using information. Developing skills and competencies in gathering and structuring data and information and in conducting detailed analysis, drawing conclusions and presenting recommendations should also be embedded in the training. Furthermore, training of analysts covers: report writing skills; the collaboration between analysis and investigations, and between analysis and decision-making; analysis methods, tools, techniques and analysis software; sources of information; evaluation codes; and legal frameworks, human rights and police ethics related to all of these tasks. Training can be presented in several phases and for different levels.

Training of investigators

Investigations include operational intelligence work. Therefore, investigators should undergo adequate ILP training before they start working on investigations. Investigators' training should include introduction to operational analysis and how it can support criminal investigations, as well as the co-operation between analysts and investigators.

Training of uniformed police

The uniformed police are in direct contact with the public and with persons involved in crime and therefore represent a valuable source of information for the intelligence sector. All uniformed officers should receive general training on ILP and its main components, including their responsibilities within the ILP model.

Training of cadets

ILP training should already be introduced during basic police training. It is particularly important to clarify all basic concepts within the ILP framework to avoid any unnecessary mystification around criminal intelligence affairs. Efforts should be made to introduce criminal intelligence work as part of normal police activities, an appealing area to future police officers.

8. ILP in practice

Previous chapters have focused on clarifying the ILP concept and the criminal intelligence analysis process, introducing some key challenges and conditions for a successful application of ILP, and presenting suggestions of an organizational set-up necessary to facilitate an effective implementation of ILP.

Chapter 8 builds on preceding chapters by offering a number of examples of ILP in practice, starting with a sub-chapter on how threat assessments play a vital role in addressing serious and organized crime. This is followed by five examples of good practices of national implementation of ILP or its key components. Finally, sub-chapters 8.3 and 8.4 present ILP and community policing, as well as ILP in preventing and countering terrorism and VERLT.

8.1 ILP, threat assessments and strategic planning in targeting organized crime

Organized crime threatens peace and human security, jeopardizes the enjoyment of human rights, and undermines the economic, social, cultural, political and civil development of societies around the world.[64] Law enforcement authorities, however, are only able to investigate a small percentage of information and intelligence they receive on organized crime and organized criminal networks in their respective jurisdictions. Therefore, assessing the seriousness of these threats and deciding on prioritization and designating available human, financial and technical resources are vital. The ILP model provides the framework needed for a modern approach and for organizational structures to adopt what is commonly recognized as the only viable option to tackle transnational organized crime, namely, data and information analysis, sharing and co-operation, addressing identified and assessed threats in a prioritized and targeted way.

64 www.unodc.org/unodc/en/organized-crime/index.html?ref=menuside

> "Serious and organized crime will remain highly dynamic and quick to exploit changes in the wider environment. Law enforcement authorities […] are challenged to keep pace with technological innovation and increasingly complex criminal ventures penetrating all sectors of the economy and society – all the while limiting their expenditure or in many cases coping with shrinking budgets. Mirroring crime, policing is becoming more complex and fighting criminals now requires an unprecedented degree of specialization and expert knowledge. Law enforcement authorities will have to find ways to reconcile budget constraints with the need for highly specialized knowledge. […]
> Advanced data analytics can help law enforcement authorities to prioritise their efforts and engage in truly smart and intelligence-led policing." **– Europol (2015: 44).**

8.1.1 The EU Policy Cycle

The EU formally endorsed ILP in 2005.[65] Since then, common EU strategic planning and operational action plans to tackle organized crime have been developed with the ILP approach. In 2010, the EU adopted the *EU Policy Cycle for Serious and Organized Crime*, which is presented here as an example of good practice for addressing transnational organized crime in line with the principles of ILP.[66]

The EU policy cycle seeks to deliver a coherent framework and robust operational actions in targeting the most pressing criminal threats facing the EU. The policy cycle provides an opportunity for, and is geared towards, integration between the different structures in a multi-disciplinary approach, including in generating synergies among law enforcement and border management authorities and facilitating further co-operation between European agencies as well as with non-EU stakeholders.

Each policy cycle covers four years in total and is comprised of four main steps, as presented in Figure 8.1.

---

65 Council of the European Union. "Council conclusions on intelligence-led policing and the development of the Organized Crime Threat Assessment (OCTA)." Doc. 10180/4/05, REV 4 (Brussels: 3 October 2005).

66 Council of the European Union. "Council conclusions on the creation and implementation of a EU policy cycle for organized and serious international crime." 3043rd Justice and Home Affairs Council Meeting (Brussels: 8 and 9 November 2010).

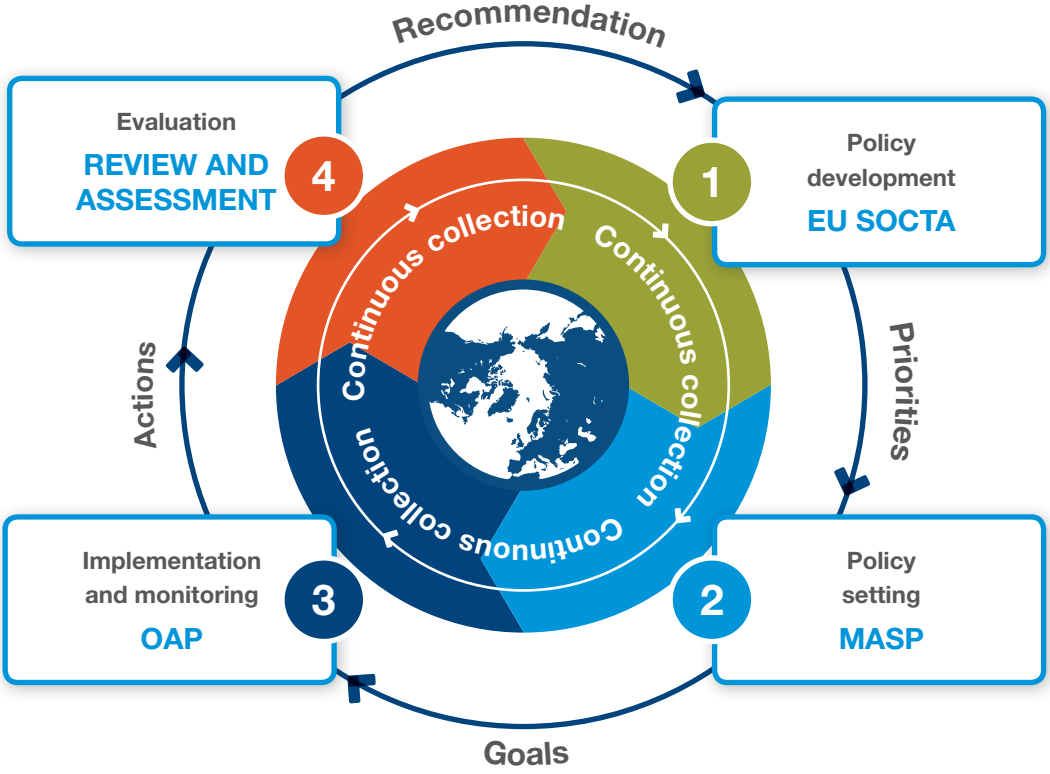


Figure 8.1 **The EU Policy Cycle to tackle serious and organized crime**
MASP: Multi-Annual Strategic Plans
OAP: Operational Action Plans
Source: Council of the European Union (2014).

STEP 1 – EU Serious and Organized Crime Threat Assessment (SOCTA)

The SOCTA is developed and published by Europol in co-operation with the SOCTA Advisory Group (composed of EU member states, EU Agencies, European Commission and Council General Secretariat), with support from Europol's third partner countries and organizations. Since the methodology is endorsed by the EU Council of Justice and Home Affairs Ministers, it has a clear legal framework and a strong political back-up.[67]

> "From strategic priorities through to operational action, [SOCTA] will ensure that an intelligence-led approach is at the heart of tackling the major criminal threats facing the EU." **– Europol (2010).**

Europol's SOCTA process includes:
- preparation and endorsement of detailed customer requirements;
- preparation and endorsement of the methodology;
- identification of intelligence requirements;
- data collection;
- analysis of data;
- drafting of the SOCTA report, including a list of key threats and risks; and
- presentation of the results and recommended priorities.

The analysis process is carried out by focusing on four elements; specific data are collected for each of them (see Table 8.1):
- serious and organized **crime areas/types**;
- organized **criminal groups/networks** and lone actors involved in serious crime;
- the **environment**: vulnerabilities, opportunities and infrastructures; and
- **effects** and **harm.**

The basic threat assessment is performed by conducting a qualitative analysis of two types of indicators, shown in the first two columns of Table 8.1. Still, a threat can only cause harm if there are vulnerabilities. Therefore, in order to provide a comprehensive assessment of the risks resulting from these threats, additional elements of vulnerability and probability/likelihood as well as effects and harm need to be identified, analysed and assessed. The public SOCTA methodology document lists the following threat and risk indicators to be assessed in the SOCTA process, shown in Table 8.1.

67 Council of the European Union. "Serious and Organised Crime Threat Assessment 2017 – Revised methodology." Doc. 14913/15, CRIMORG 128 (Brussels: 11 December 2015).

Table 8.1 **The set of indicators analysed during the SOCTA process**

THREAT ASSESSMENT		THREAT + RISK ASSESSMENT	
Crime areas/types	Criminal groups/ networks	Environmental crime relevant factors	Effects/harm
Availability of resources	Crime areas/types they are active in	Economic situation	Financial impact
Demand and supply	Poly-crime activities	Geopolitical situation	Social impact
Number of groups active in the crime area/type	Nationality	Transport and logistics infrastructure	Health impact
Evolution of the crime area/type	Size of the group	Public attitudes	Environmental impact
Geographical dimension	Financial resources	Innovation	
Other crime areas/ types linked	Human resources	Internet and new technologies	
Modus operandi used	Financial profit	Legislation	
	Other resources	Law enforcement action	
	Structure, type	EU crime priorities set by the Committee on Operational Cooperation on Internal Security (COSI)	
	Expertise		
	Co-operation		
	Modus operandi		
	Geographical dimension		
	Flexibility and adaptability		
	Counter-measures		
	Corruption and influence in the public sector		
	Use of legal business structures		
	Money laundering – level of sophistication		
	External violence		

Threat assessments are not descriptive reports of the present state of play, but are forward-looking. They present conclusions with a list of key threats and recommendations on how to prioritize them. Europol SOCTA reports are submitted to the EU Standing Committee on Operational Cooperation on Internal Security (COSI) where they are discussed within the political EU policy-making process. Thus, the final decision is a mixture of professional experts' assessments and political views.

STEP 2 – The Multi-Annual Strategic Plans

Based on the SOCTA, the EU Council of Justice and Home Affairs Ministers makes a formal decision on priority crime areas for the next four years. When setting these policies, the Council takes into account comments from EU member states, agencies and partner non-EU countries.

For each of the priorities, an expert group from the most affected countries drafts a four-year Multi-Annual Strategic Plan (MASP). These multi-disciplinary plans contain a list of strategic goals that should be achieved during the four-year cycle. Key performance indicators, timelines, milestones and responsible agencies/persons are included in all the plans. COSI adopts the MASPs, giving them a formal status and securing financial resources.

STEP 3 – Operational Action Plans and the European Multidisciplinary Platform Against Criminal Threats (EMPACT)

Each MASP is developed into an Annual Operational Action Plan (OAP) per priority. All OAPs describe steps and actions of EU institutions and agencies as well as action that will be carried out by single national authorities.

Joint actions within the OAPs are executed within the European Multidisciplinary Platform Against Criminal Threats (EMPACT) mechanism. This mechanism provides a structured co-operation platform for the relevant member states, EU institutions and agencies, as well as involved non-EU partners. The implementation of each OAP is led by a volunteering driver from an EU member state, and the implementation is overseen at the national level by National EMPACT Coordinators (NECs), designated in each EU member state. Europol provides administrative and logistical support to the EMPACT projects and monitors their progress. Europol also designates EMPACT Support Managers to ensure analytical and operational support to all crime priorities. COSI approves the OAPs and monitors their implementation on the basis of reports every six months.

All EU national authorities are invited and encouraged to integrate the MASPs and OAPs into their national planning processes and their law enforcement efforts to counter serious and organized crime. Relevant EU agencies are also encouraged to reflect priorities and action plans into their yearly work programmes.

STEP 4 – Review and assessment

The effectiveness of the OAPs and their impact on the priority threats will be reviewed by COSI. Annual reporting by the national drivers and an interim assessment by Europol provide opportunities to adapt or modify the MASPs, or the priorities if necessary. COSI receives

a yearly state of play and conducts a thorough and independent evaluation at the end of each policy cycle. The lessons learned from this evaluation serve as input for the next policy cycle.

8.1.2 The Sleipnir Organized Crime Assessment Tool

The Sleipnir technique was developed to improve strategic priority setting by providing a reliable, objective, expertise-based method in criminal intelligence analysis to assist in the ranking and comparison of the threat of organized crime groups as well as to identify intelligence gaps.

The Sleipnir technique provides intelligence analysts working on organized crime groups with a comprehensive and transparent method to develop and present recommendations and supporting intelligence in a concise manner. However, the resulting framework and matrix are not intended to stand in isolation, but should be fleshed out in the context of a strategic analytical assessment that explains the details and significance of the comparisons.[68]

Originally, there were 19 criteria or attributes by which relative levels of threat were assessed. All attributes are assigned a value – either "unknown", or from "nil" to "high" – based on their observed magnitude, but an updated version of the Sleipnir technique has reduced the number of attributes down to 12. This made the information collection process more efficient, while the remaining attributes would focus on more easily observable behaviour.

However, it should be understood that Sleipnir is a strategic tool used to assist in determining organizational priorities and is not designed to be used as a tactical intelligence tool. The Sleipnir technique is also grounded in certain assumptions that may not reflect the increasingly complex and sophisticated links between international organized crime groups, and between these groups and terrorist organizations. This could lead to the development of strategic priorities that focus too much on large, sophisticated organizations while ignoring smaller and potentially more dangerous groups with links to foreign organized crime or terrorism.[69] In addition, Sleipnir is based on assumptions that determine the greatest perceived threats to Canadian society, and the rank ordering of attributes may not necessarily reflect those relevant to other societies or jurisdictions.

68 Royal Canadian Mounted Police Criminal Intelligence. "Sleipnir Version 2.0, Organized Crime Groups Capability Measurement Matrix." Royal Canadian Mounted Police (Ottawa, 2011).

69 Ratcliffe, Strang and Taylor (2014: 206-227).

Table 8.2 **A comparison of five crime groups using the Sleipnir model**

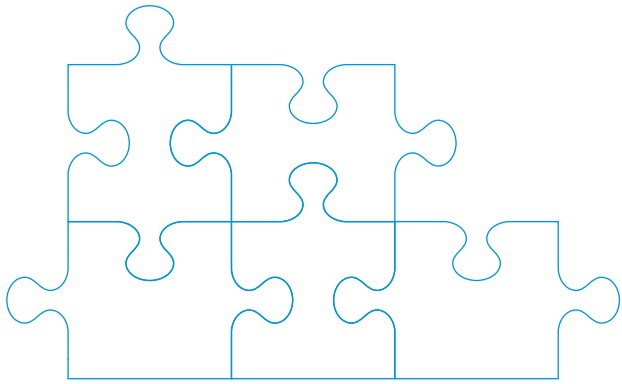
	GROUP 1	GROUP 2	GROUP 3	GROUP 4	GROUP 5
Corruption					
Violence					
Infiltration					
Money laundering					
Collaboration					
Insulation					
Monopoly					
Scope					
Intelligence use					
Diversification					
Discipline					
Cohesion					

DEGREE OF THREAT	
High	
Medium	
Low	
Nil	
Unknown	

The key difference between the threat categories 'nil' and 'unknown' is whether or not information was collected on the group. If a group has not been investigated or the subject of criminal intelligence, the attributes with no information should be scored as 'unknown'. 'Unknown' should also be used when there is reason to suspect that a group has a capability of posing a threat, but no proof that they are using its capabilities, and when there is conflicting information available on it capability with insufficient certainty to support a judgment.[70]

Sleipnir sub-components

There are 12 attributes or 'values' in the Sleipnir tool, which correspond to the threat they pose to Canadian society. In the tool, they are ranked from biggest threat to smallest threat to a society. For instance, 'corruption' is considered the largest threat from organized crime, followed by 'violence'.



70 RCMP. "Sleipnir Version 2.0". (2011: 2).

Below is the rank-ordered list that describes the 12 values (P, see below) used to score different crime groups:

12. Corruption
11. Violence
10. Infiltration
9. Money laundering
8. Collaboration
7. Insulation
6. Monopoly
5. Scope
4. Intelligence use
3. Diversification
2. Discipline
1. Cohesion

Scoring

Each of the 12 values can be scored using the following method:

- High = 4 x P
- Medium = 2 x P
- Low = 1 x P
- Nil = 0
- Unknown = 2 x P

Where P is the number of the subcomponent in the list above; for instance, if Monopoly (#6) is high, Intelligence use (#4) is medium, and Violence (#11) is low, they would be scored in the following way:

- Monopoly = 4 x 6 = 24
- Intelligence use = 2 x 4 = 8
- Violence = 1 x 11 = 11

The total will be 43. A higher score, relative to other organizations being checked, represents a higher level of threat.

8.2. National ILP implementation examples

Sub-chapters 8.2.1 to 8.2.5 provide examples of implementation of ILP in five countries in Europe. Sub-chapter 8.2.1 begins by introducing the National Intelligence Model (NIM) in the United Kingdom (UK), where ILP was first developed in the 1990s. The UK ILP practical application and organizational structures have since then been used as a good practice model by many countries around the world. The NIM is followed by a brief presentation of the intelligence-led policy-making and strategic planning of law enforcement in the German State of North Rhine-Westphalia. Sub-chapter 8.2.3 presents the Swedish ILP model as well as intelli-

gence-based Joint National Efforts in addressing serious and organized crime in Sweden. The Republic of Serbia integrated specific legal provisions on ILP in a new Police Act adopted in 2016 and developed a National Handbook on ILP for the Serbian law enforcement services. These measures are introduced in sub-chapter 8.2.4. The last national example describes the Montenegrin approach to threat assessments of serious and organized crime.

8.2.1 The UK National Intelligence Model

The NIM is the implementation framework of ILP in the UK.[71] The intention behind the NIM is to provide focus to operational policing and to achieve a disproportionately greater impact from available resources. It is based on a clear framework of analysis of data and information, allowing a problem-solving approach to law enforcement and crime prevention techniques. The expected outcomes are improved community safety, reduced crime, and the control of criminality and disorder leading to greater public reassurance and confidence. The NIM is not confined or restricted to specialist usage. It is relevant to all areas of law enforcement: crime and its investigation, disorder and community safety. Overall, the NIM is a business model for operational policing.

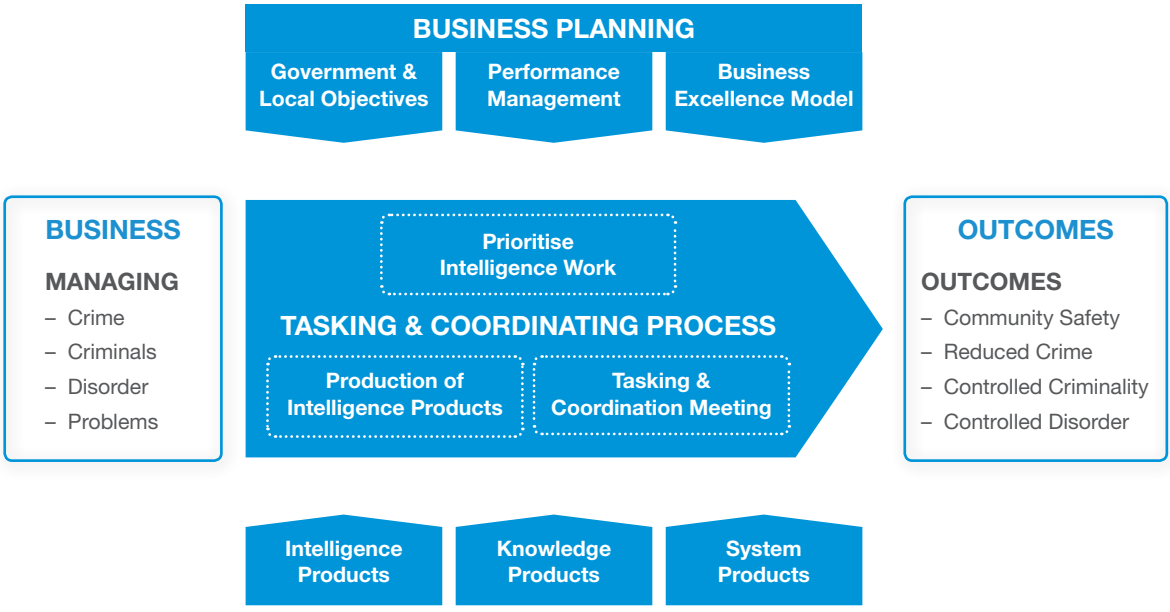


Figure 8.2 **The UK National Intelligence Model**

Source: NCIS (2000: 9).

71 This sub-chapter is drafted on the basis of two documents: *(i) The National Intelligence Model* of the Criminal Intelligence Service (NCIS) (NCIS Corporate Communications, 2000); and (ii) the *Code of Practice – National Intelligence Model* of the National Centre for Policing Excellence (London Home Office, CENTREX, 2005).

The NIM is as much a management decision-making model as a description of intelligence processes and products. The critical factor in securing reduction in crime is the proactive role of law enforcement management.

The process is conducted at three levels: Level 1 (community/local level), Level 2 (inter-force/regional) and Level 3 (national/international).

At each of these levels, the processes and nature of the intelligence products are essentially identical, although the detailed content of the products and the nature of the data to be accessed and processed will vary. This similarity throughout the model is deliberately highlighted to broaden understanding among professionals working at different levels.

The NIM works either as a stand-alone system for one level of activity, or as an integrated model whereby at each level it interacts with the others to best identify the problems and their potential solutions. The model describes each intelligence unit within a level, setting its own local intelligence requirement. The standardization of intelligence products will provide the best basis for providing such intelligence, but it requires systems of access that enable each intelligence unit to benefit from the data held by its colleagues.

The pivotal product at Level 3 is the UK Annual Threat Assessment, more precisely titled *The National Strategic Assessment of Serious and Organised Crime* (NSA). It is produced by the UK National Crime Agency (NCA) drawing on data provided by the police forces, HM Customs and Excise, the intelligence and security agencies, and other law enforcement bodies.

The NSA provides a comprehensive picture of the risk posed to the UK and its interests by serious and organize crime. It provides the national response with information on what the priorities are and what action will be taken the expected results and how success will be measured.

Tasking and Co-ordination Groups, which meet on all three levels, are at the heart of the NIM. Meetings of these groups are divided into *Strategic Tasking and Co-ordination Meetings* and *Tactical Tasking and Co-ordination Meetings*. The purpose of these meetings is to agree on a Control Strategy that establishes the intelligence requirement and sets the agenda for intelligence, prevention and enforcement priorities, aiming at a maximum impact. To this end, law enforcement managers must have a good understanding of the true nature of the problems they face and a mechanism for decision-making that identifies priorities, the resources required and which can commission action. The tasking and co-ordination process is that mechanism.

TASKING AND COORDINATION

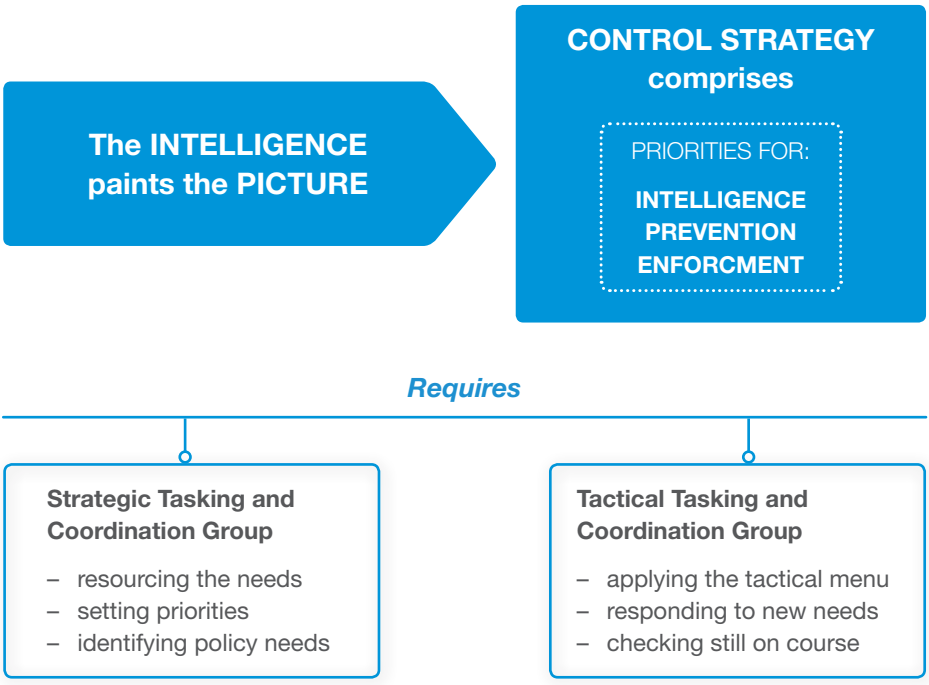


Figure 8.3 **Strategic and Tactical Tasking and Co-ordination processes in the United Kingdom**

Source: NCIS (2000: 14).

Strategic tasking

The objectives of the *Strategic Tasking and Co-ordination Meetings* are to set up or amend the control strategy and to make the principal resource commitments in line with set priorities. The Strategic Tasking and Co-ordination Group therefore meets quarterly or half-yearly and aligns its cycle to the business planning round. The Group's work is carried out on the basis of the problems and issues identified by the Strategic Assessment (NSA), which, having been considered in light of the governmental and local objectives, is used to determine and set the priorities for intelligence, enforcement and prevention. Its work is completed by the allocation of resources and setting of policies needed to deliver the control strategy.

Tactical tasking

The *Tactical Tasking and Co-ordination Group* meets weekly or every second week. It has three main roles: to commission and apply the tactical menu to the Control Strategy; to respond to new needs; and to check that agreed plans and enforcement work are still on course to meet objectives. A Tactical Assessment Report is the key intelligence product that drives the tactical decision-making.

The tactical aims comprise four elements:

- targeting of offenders in line with the priorities of the Control Strategy;
- the management of crime and disorder hotspots;
- the investigation of crimes and incidents which can be shown to be linked into 'series';
- the application of the range of "preventative measures" such as CCTV and lighting schemes or community action initiatives.

Monitoring the progress and encouraging work in the four boxes of the tactical menu is the heart of the agenda for the Tactical Tasking and Co-ordination Meeting.

The intelligence-led strategic and tactical tasking and co-ordination processes are based on four main intelligence reports briefly explained below.

Strategic assessments

The main purpose of the strategic assessment report is to give the Tasking and Co-ordination Group an accurate picture of the situation in its area of responsibility, and how this picture is changing and may change in the future. It is by definition a longer-term, high-level look at the law enforcement issues and will therefore not only consider current activities, but will also try to provide a forecast of likely developments. A locally produced strategic assessment will assist planning and policy-making in the area and contribute to the bigger picture of patterns and trends in the region and nationally.

Tactical assessments

The tactical assessment forms the basis for the work of the Tactical Tasking and Co-ordination Group. The assessment will be able to identify emerging patterns and trends requiring attention, including further analysis. Progress in investigations or preventive initiatives can be addressed as can immediate needs for changes in resourcing tactical options.

Target profiles

A target profile is person-specific and contains sufficient detail to initiate a target investigation/operation or support an ongoing operation against an individual or networked group of individuals. It shows links to other investigations (at all levels of the model) and may include risk profiles of potentially dangerous offenders. On the basis of the intelligence revealed, the target profile includes an interpretation of the best course of action and proposals to fill the gaps in the intelligence picture.

Problem profile

A problem profile identifies established and emerging crime or incident series. It also identifies established and emerging crime and incident 'hotspots' together with the opportunities for preventive work revealed by the intelligence. In the case of crime series identification where methods are confirmed and links to potential offenders established, the profile supports targeting and reactive investigation, as well as preventive initiatives.

Intelligence Units – prioritization of intelligence work

An effective and secure intelligence unit needs four main assets briefly described below: adequate *sources of information*, appropriately organized and skilled *staff*, access to the range of *knowledge products* and *system products*.

Sources of information

The sources that intelligence staff need to access are wide-ranging, such as victims, witnesses, prisoners, informants and surveillance products. A soundly equipped intelligence regime will be able to access a wide range of existing data as well as undertake proactive source recruitment and deployments to fill identified intelligence gaps.

Staff

The second asset required is people. It is vital that an intelligence manager of appropriate status be appointed to head the unit to ensure that meaning and significance are added to the analytical techniques and products before they are presented to the tasking and co-ordination group.

It is equally important that intelligence as a discipline be adequately represented in management discussions about financial and human resources. Intelligence units need to be equipped not just to handle data and information that is already known, but also to gather information through proactive or covert means. Gaps in intelligence will often be identified that cannot be filled by analysis and collation of available material. Intelligence units must have the skills and capability to handle live sources, as well as opportunities for technical surveillance operations.

Trained analysts are required if the standards inherent in the model are to be reached. The analytical techniques and products are part of a standard range that underpins the national vocational training arrangements for law enforcement analysts.

Knowledge products

The model asserts that the intelligence discipline has to be learned. Staff need access to the knowledge products that provide quality assurance to the model. These knowledge products, national and local, define the rules of conduct of the business or the best practice by which skilled processes are completed, and the conditions in which work between agencies may take place. Access to the knowledge products makes staff fit for their roles. Therefore, the term knowledge products describes a variety of local, regional or national rules and information that an organization's intelligence strategy may need to embrace.

System products

System products are enabling facilities for the collection, reception, recording, storage and use of information. They provide the means by which data is held, retrieved and analysed. According the NIM, effective intelligence units need access to a number of national data systems, local police force case files, crime and intelligence records and the wide variety of open source information.[72]

72 For detailed information on system products for intelligence units, see NCIS (2000).

Security

The integrity of the NIM requires adequate standards of physical, environmental, technical and personnel security. The Government Security Classifications policy sets out common standards for the protection of sensitive documents and other material across all government agencies. Its principles also extend to data held on computer and electronic recording systems.

Data protection

Chief Officers are responsible for the development and implementation of appropriate procedures and systems to ensure that personal information on individuals is held in accordance with the requirements of the UK Data Protection Act 1998 and any other relevant legislation. The management of information must be in accordance with the Code of Practice on Management of Police Information.

8.2.2 North Rhine-Westphalia, Germany: Policy-making and strategic planning

The State Police of North Rhine-Westphalia in Germany applies ILP, including in policy-making and strategic planning.[73] The strategy management and controlling system is based on four pillars representing the State Police force's core tasks:

- Danger prevention and emergency response (DE)
- Combat crime (Investigations)
- Combat traffic accidents (Traffic)
- Administrative services (AS).

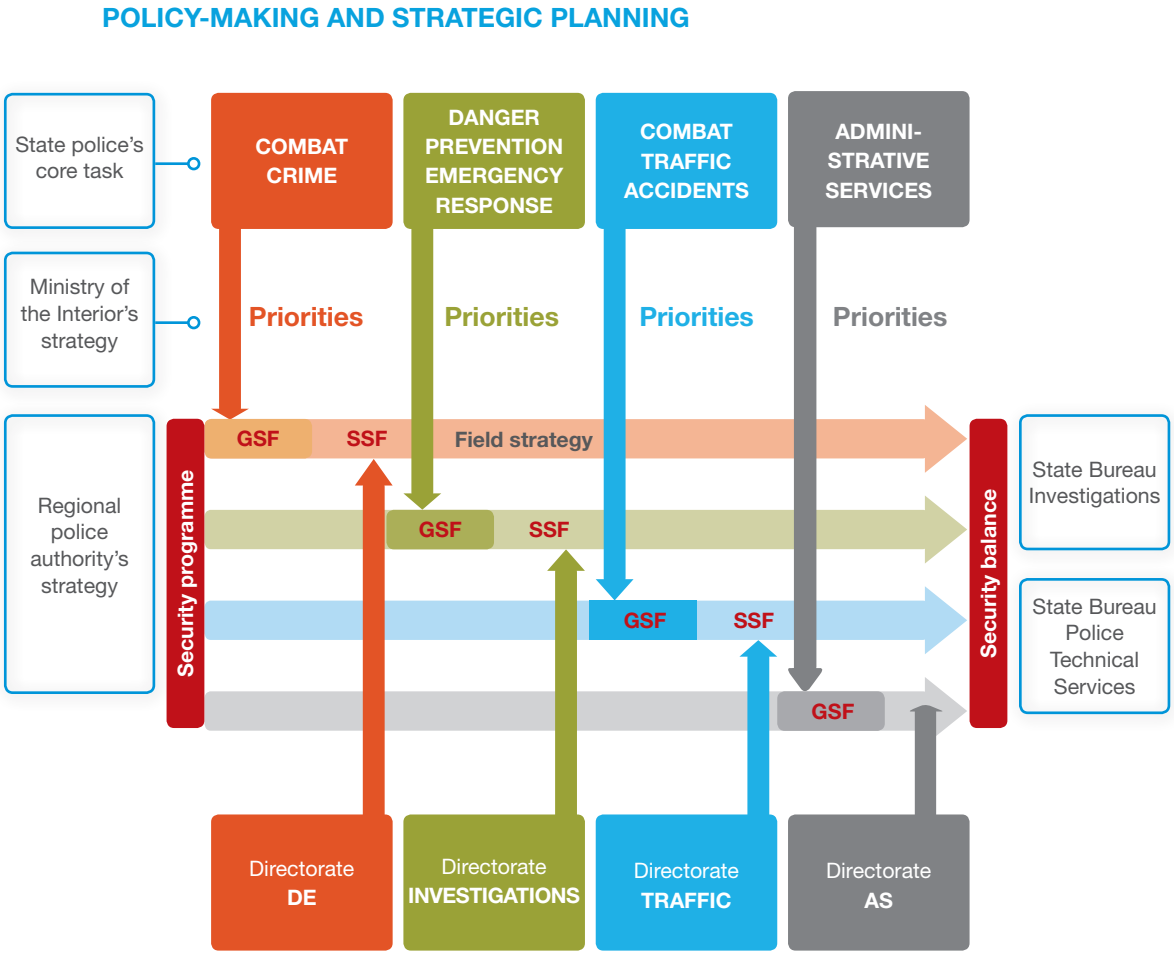
All 47 Regional Police Authorities (RPAs) in North Rhine-Westphalia (NRW), although different in size, have an identical organizational structure, which consists of four directorates corresponding to the core tasks and an additional staff, supporting the head of the police authority.

As a strategic base, the Ministry of the Interior (MoI) identifies state-wide priorities in each field of the four above-mentioned pillars (field strategies). They are generated, periodically evaluated, and adjusted by analysis of information and data, collated and cross-checked by two state agencies. This process also determines a load-related resource allocation and budgeting for the RPA.

Examples of potential priorities:

- (DE) Availability and accessibility the Police;
- (Investigations) Reducing juvenile crime;
- (Traffic) Reducing accidents of elder people;
- (AS) Availability of personnel within the RPA.

73 Responsible authority: Landesamt für Zentrale Polizeiliche Dienste NRW, Duisburg, Germany.



GSF: General Success Factors
SSF: Special Success Factors

Figure 8.4 **Intelligence-led policy-making and strategic planning of the State Police of North Rhine-Westphalia, Germany**

For each of the priorities, the MoI defines **General Success Factors (GSFs)**, which contain a set of standards, procedures and indicators whose application is mandatory for all RPAs. They have to be included in the RPA's annual **Security Programme**, which also describes the RPA's local priorities and objectives, and related measures and responsibilities. The binding regional standards, procedures and indicators are referred to as **Specific Success Factors (SSFs)**. Each RPA directorate is generally obliged to contribute to the achievement of the remaining three directorates' objectives.

On behalf of the Ministry, the two state agencies (State Bureau Investigations and State Bureau Police Technical Services) are tasked with periodically controlling and evaluating the RPA field activities, also documented in the RPA's year-end Security Balance. Layout and structure of both the Security Programme and the Security Balance are prescribed and identical for all RPAs. They form the basis for a feedback and intervention process including, *inter alia*, promoting and supporting examples of best practices. In assistance, comparison groups of the RPAs with corresponding structural data have been developed to enable and intensify the exchange of experience.

Advantages of the described model:

- a concentration on core tasks with regard to limited resources and budget;
- enhancement of RPA local ownership and responsibility while taking into account state-wide objectives;
- standardization of a state-wide reporting and controlling system; and
- better comparability between the RPAs.

8.2.3 Sweden: ILP organization and decision-making structures

The Swedish Police underwent major reforms in 2015, from being 21 independent Police Authorities, each led by a governance structure at the Swedish National Police Board, to a single National Police Authority, headed by a National Police Commissioner, divided into seven police regions and the National Operations Department. These organizational changes included creating a new structure and co-operation and co-ordination processes for ILP in Sweden at the national strategic level, national operational level, regional strategic level, regional operational level and local operational level. The organizational structure of the Swedish ILP model is a top-down command and control structure. All meetings of management groups of each level are attended by a representative from the next level below in order to secure co-ordination and information sharing between the levels.

The *National Strategic Management Group* (SLG) is chaired by the National Commissioner of the Police. Other representatives are the seven regional police commissioners, the head of the National Operations Department and heads of other national departments, including finance, communication and human resources. SLG has video meetings every second week but traditional meetings every month. The main responsibilities for SLG are to discuss and make decisions on national strategic directions and plans, and decide on long-term priority areas including resource allocation, based on governmental decisions, strategic reports and assessments.

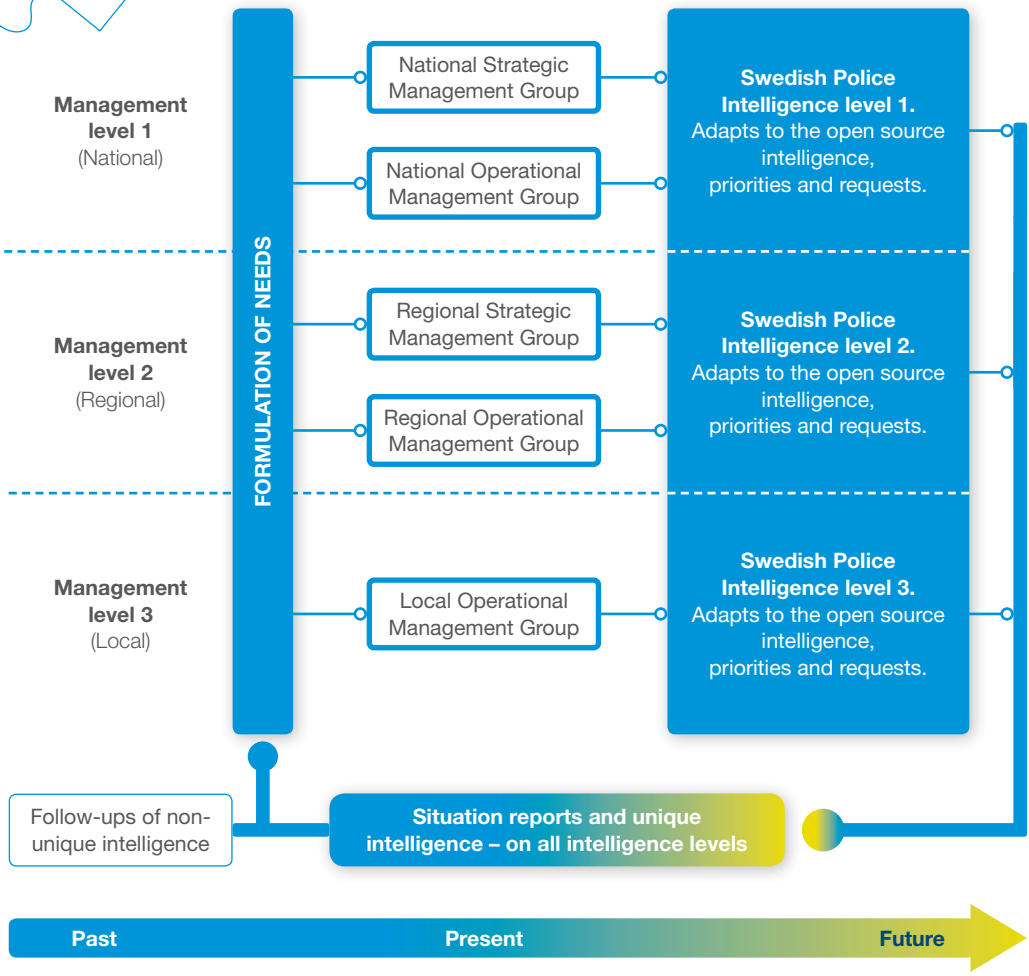


Figure 8.5 **Organizational and decision-making structures of the Swedish ILP model**

The *National Operational Management Group* (NOLG) is chaired by the head of the National Operations Department. Other representatives are the deputy heads of the seven police regions, the head of the National Operational Planning Division and the head of the National Forensic Department. The Operational Head of the Swedish Security Service and the head of the National Public Prosecution Department from the Swedish Prosecutors Authority attend meetings as observers. The NOLG has video meetings every second week and traditional meetings every month. The main responsibilities of NOLG are to prioritize national actions, operations and investigations, based on intelligence reports from the National Criminal Intelligence Unit located within the National Operations Department of the Swedish National Police Authority.

Regional Strategic Management Groups (RSLGs) are chaired by the regional police commissioners of each of the seven police regions. Other representatives are the heads of each of the police areas of the region and the heads of human resources, finance, communication, development, and investigation and operation regional units, among others. The RSLG have meetings every second week. The main responsibilities for RSLG are to discuss and make decisions on regional strategic directions and plans, and decide on long-term priority areas including resource allocation, based on national decisions by NOLG, strategic reports and assessments.

Regional Operational Management Groups (ROLGs) are chaired by deputy heads of each of the seven police regions. Other representatives are the chairs of the Operational Local Groups (POLGs) in each of the police areas in the region and the heads of regional investigation and operations units, among others. The head of each regional intelligence unit acts as the rapporteur of the ROLGs, which meets every second week. Their main responsibilities are of the ROLG are to prioritize regional actions, operations and investigations, based on available information and intelligence reports from the regional intelligence units. The ROLG can make a decision to direct proposed actions to the local level and can request operational and intelligence support from the national level (NOLG).

POLGs are chaired by the local police commissioners. Other members are the heads of sub-local police areas and the heads of local investigations and operations. Heads of local intelligence groups act as the rapporteurs of the POLG, which meets once a week. The main responsibilities of the POLG are to make decisions on local actions, operations and investigations based on reports from the local Intelligence Unit. POLG can request operational and intelligence support from the regional level (ROLG).

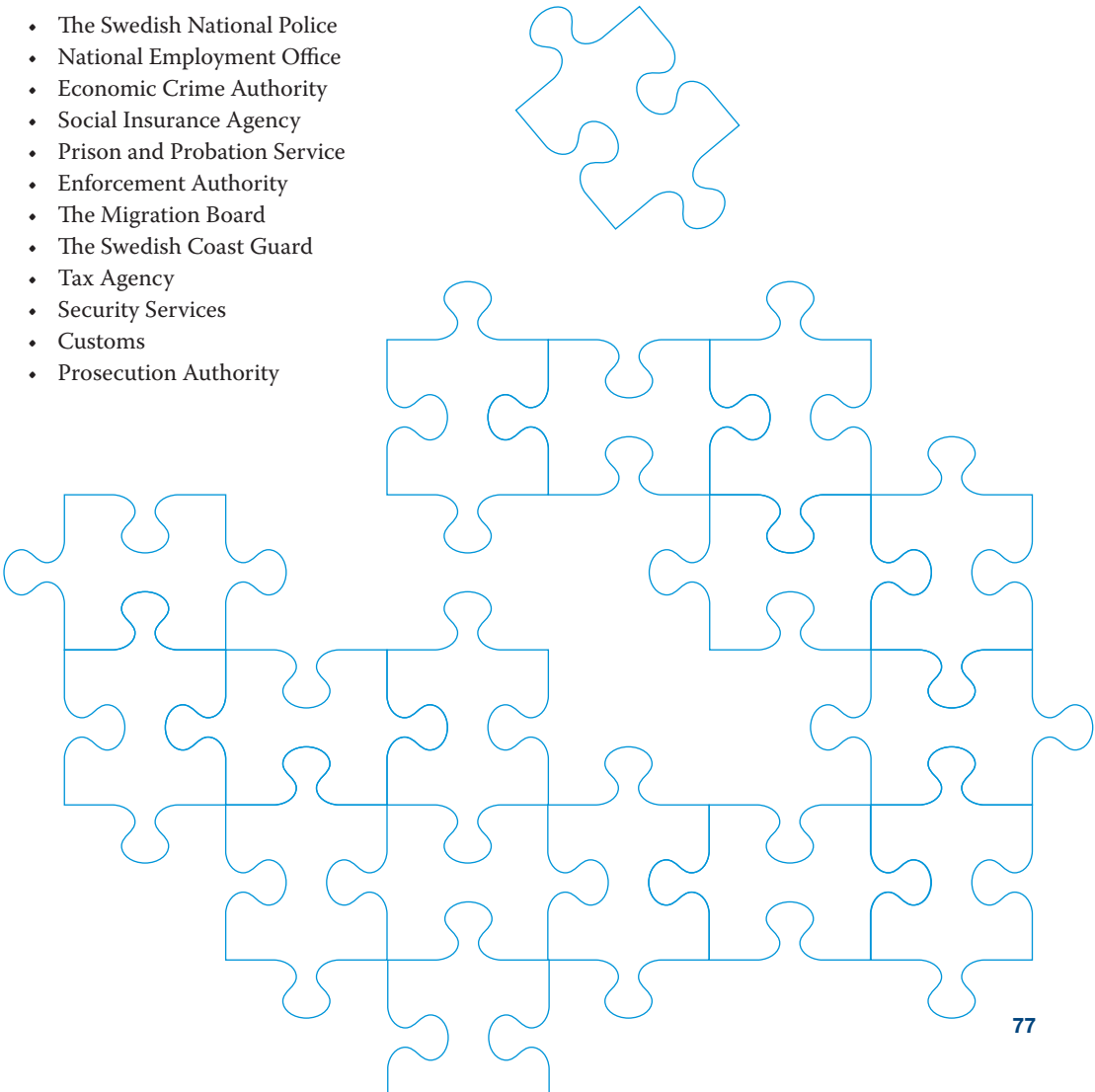
Joint National Intelligence and Operational Efforts in Sweden to address organized crime

In 2009, nine Swedish public authorities signed a co-operation agreement to launch joint intelligence and operational efforts to prevent and tackle organized crime. This national initiative was expanded in 2016 to be implemented on the regional and local levels. It runs parallel to and is directly linked to the ILP implementing structures described above.

These joint actions are specific intelligence, operational and investigative measures, but they only represent one part of the general efforts of the Swedish Police Authority and the collaborating authorities to counter organized crime.

The following 12 national agencies/authorities participate in and contribute to the joint efforts against organized crime:

- The Swedish National Police
- National Employment Office
- Economic Crime Authority
- Social Insurance Agency
- Prison and Probation Service
- Enforcement Authority
- The Migration Board
- The Swedish Coast Guard
- Tax Agency
- Security Services
- Customs
- Prosecution Authority



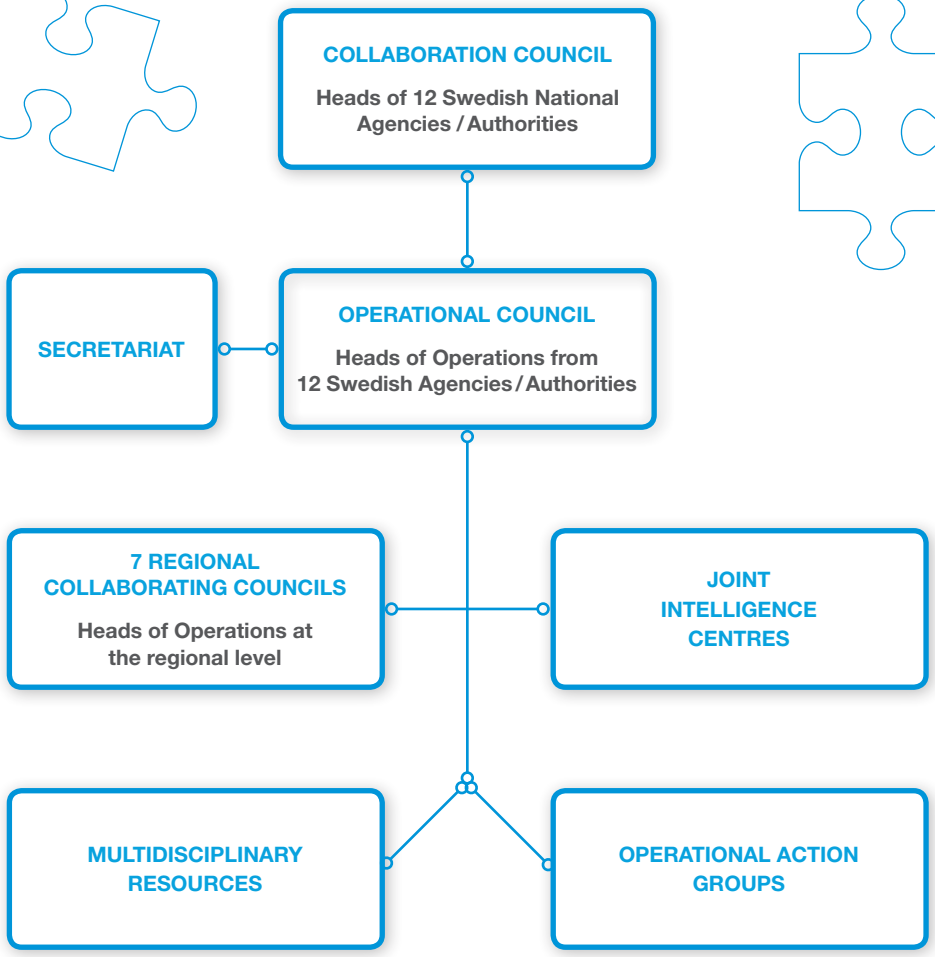


Figure 8.6 **The joint national intelligence and operational efforts in Sweden to address organized crime**

All of these 12 national agencies participate and co-operate in a multi-agency forum, the *Collaboration Council*, composed of heads of each collaborating agency/authority and chaired by the Swedish National Police Commissioner. The primary task of this Council is to make decisions on a joint strategy to address organized crime in Sweden. The Council meets twice a year. For co-ordination and information-sharing purposes, the head of the next structure below (Operational Council) acts as rapporteur.

Under the Collaboration Council is the *Operational Council*, whose main tasks are prioritizing and operationalizing strategic decisions made by the Collaboration Council. The Operational Council, which meets every month, also makes decisions on the use of Operational Action Groups and other resources in joint investigative or operational tasks. Each of the 12 agencies/authorities has one representative in the Operational Council, which is chaired by the head of the National Operations Department from the National Police Authority, thus connecting the two structures and securing information flow.

The *Secretariat* supports the collaboration and operational councils and its processes. Its main tasks are to plan, prepare and put forward proposals for decisions, take minutes and ensure follow-up of the meetings of the Collaboration and the Operational Councils. The Secretariat also has a co-ordinating role and is responsible for the process concerning the action groups.

Regional Collaborating Councils in all seven regions of the country have the main tasks of setting up joint actions at the local and regional levels. They have meetings every four weeks and report back to the Operational Council through the Secretariat.

All entities within the joint efforts are supported by intelligence structures comprised of multi-agency *Regional Intelligence Centres* located in the seven police regions, and a multi-agency *National Intelligence Centre* located at the National Operations Department. These centres, represented by 11 of the collaborating agencies/authorities,[74] provide the joint efforts with analytical services and intelligence products. According to law from 2016, all these agencies/authorities are not only allowed, but obliged to share each other's data, information and intelligence on intelligence tasks, conducted within the forum, when addressing criminal activity of serious nature, conducted in an organized manner and systematically by a group of individuals.

The Operational *Actions Groups* are composed of around 200 law enforcement staff. The groups are divided in sections of 20 or 30 officers, located in the seven police regions and at the National Operations Department. Each unit has a head/group leader, investigators, analysts and administrators. The actions groups also collaborate with other *multidisciplinary resources* from other co-operating authorities on daily basis as joint teams in actions decided by the Operational Council.

74 The Swedish prosecution authorities are not represented in the Joint Intelligence Centres as prosecution authorities do not possess or handle intelligence.

8.2.4 Republic of Serbia: Operational and intelligence structures of ILP

The Ministry of Interior of the Republic of Serbia decided to implement the ILP in Serbia to improve law enforcement and bring results in combating crime and other security threats to a higher level, as well as to align police work with the standards, structure, quality and terminology of the police forces in developed countries in Europe and the world. In this regard, Serbia adopted a new Law on Police in 2016, which defines ILP and provides instructions on how to apply it in Serbian policing practice.

Serbian Law on Police

Article 34
Police intelligence model

> "In the performance of police tasks, the Police shall apply the intelligence-led policing (ILP) model. Intelligence-led policing is a model of managing police work based on criminal intelligence. Criminal intelligence is a set of collected, evaluated, processed and analyzed data, as a basis for making informed decisions relating to the performance of police tasks."
>
> **– Ministry of Interior of the Republic of Serbia. "Decree on the Promulgation of the Law on Police." PR No. 1, Belgrade, 28 January 2016.**

The Serbian Law on Police also defines and clarifies the roles and responsibilities of the different police structures and levels in managing key elements of the ILP model, including developing a Strategic Assessment of Public Safety, as well as strategic and operational plans, which define the priorities and objectives of police work, based on the Strategic Assessment.[75]

Following an in-depth study of developed ILP models, such as the United Kingdom, American, Canadian, Australian, and Swedish models, the Ministry of Interior developed a Serbian ILP model, which is fully adapted to the specificities of the police system in the Republic of Serbia. The Serbian ILP model is described in the Serbian National ILP Handbook[76] and includes the following chapters:

- Structure of the ILP Model in the Republic of Serbia
- Leading and Steering on Strategic and Operational Levels

75 Serbian Law on Police (2016): Art. 24 (role and responsibilities of the Police Directorate within the Serbian Ministry of Interior); Art. 25 (main tasks and activities of police departments).

76 Ministry of Interior of the Republic of Serbia (2016).

- The Criminal Intelligence Process and Practices
- Criminal Intelligence Work (planning, collecting, processing, analysis and dissemination intelligence)
- Planning of Operational (executive) Police Work
- Security and the ILP Model
- Employees and Units responsible for Criminal Intelligence Affairs
- Staff Development and Training
- Information and Communication Systems.

In the Serbian Handbook, the term "intelligence-led policing" refers to a system and methodology for managing criminal intelligence and planned operational police work, in which intelligence is the basis for defining priorities, strategic and operational objectives in the prevention and suppression of crime and other security threats. It is also the basis for making appropriate decisions on operational police work and actions, rational engagement of available human resources, and for the allocation of material and technical resources.

The Serbian Ministry of Interior is currently implementing ILP model in policing practices in Serbia. The Swedish Police Authority and Swedish International Development Cooperation Agency have been providing support to the Serbian police in the implementation process from the beginning. In order to design the described Serbian ILP model, a gap analysis was conducted to identify concrete activities that need to be undertaken in the areas of adjusting the legal framework, the organizational structure, the development of human and IT capacities. Several regulatory documents pertaining to ILP have been adopted. The Strategic Assessment of Public Safety covering a period of five years and the National SOCTA have been adopted. Human resources tasked with implementing ILP have also been allocated. The plan is to have ILP fully implemented by the Ministry of Interior of the Republic of Serbia in 2018.

The Serbian ILP is a model designed to manage all police work, not just police work focusing on prevention and suppression of organized crime.

Necessary conditions for effective functioning of the ILP model, according to the Serbian Ministry of Interior and the Serbian ILP Handbook are:

1. *Leading and steering* – This is a key function of the model that is established on a strategic and operational level and is performed in accordance with an established methodology and system of responsibility.

2. *Systematized criminal intelligence process* – The complete criminal intelligence process in practice must be structured into sub-processes (tasks), functions and activities that are either mutually connected or take place at the same time.

3. *Effective organizational structure* – Organizational units and sub-units that are engaged in criminal intelligence and operational police work are established so as to be compatible with defined processes and functions (similar processes and functions are performed within the same organizational units).

4. *Sources of data and information* – All available open and closed sources must be identified and efficiently used with the aim to collect data and information.

5. *Focus on the most difficult security problems* – Organized crime, corruption and other serious criminal offences and perpetrators (organizers and executors) should be prioritized.

6. *Criminal intelligence products* – In accordance with the defined methodology for the performance of criminal intelligence work and defined quality criteria, the Unit for Criminal Intelligence Affairs produces criminal intelligence products, which are a pre-requisite in properly defining objectives, determining priorities and decision-making for the performance of police work.

7. *Legal framework* – A suitable legal framework must be defined for ILP to operate successfully.

8. *Human resources* – Police officers should be specially selected (in accordance with special criteria and procedures) and trained in the performance of criminal intelligence work.

9. *Technical resources* – Developed databases and information technology, adequate premises, technical equipment and tools are necessary elements of the ILP model.

10. *Time as a resource* – It takes time and patience to change the organizational culture and way of working.

As shown in Figure 8.7, the ILP implementation process consists of three sub-processes, representing the flow of activities in the shape of the number eight. These sub-processes are: (i) leading and steering (blue); (ii) criminal intelligence work (white); and (iii) planned operational police work (red). The mid-level sub-process, leading and steering, plays a managerial (directing and co-ordinating) role with respect to the other two sub-processes. *First,* within the sub-process leading and steering, competent managers initiate (request) the implementation of criminal intelligence work. Based on their tasking and requests, concrete intelligence activities are planned and carried out, and the results presented a report. *Second,* on the basis of this report, the competent managers make decisions on the implementation of planned operational police work. *Third,* based on these decisions, concrete operational police activities are planned and carried out, and followed by an evaluation report. The described flow of the criminal intelligence process (white) can either end after one cycle or be repeated (completed with new additions) in several cycles depending on the success rate of solving a particular crime and on other circumstances.

Figure 8.7 **The Serbian ILP model.**

Source: Ministry of Interior. Republic of Serbia.

The Serbian ILP organizational structures divide decision-making, leading, steering and co-ordination into three levels: national, regional and local. In line with the ILP principles, each level has its decision-making mechanism based on strategic and operational criminal intelligence products, thus incorporating analysis and assessments into all law enforcement planning and management:

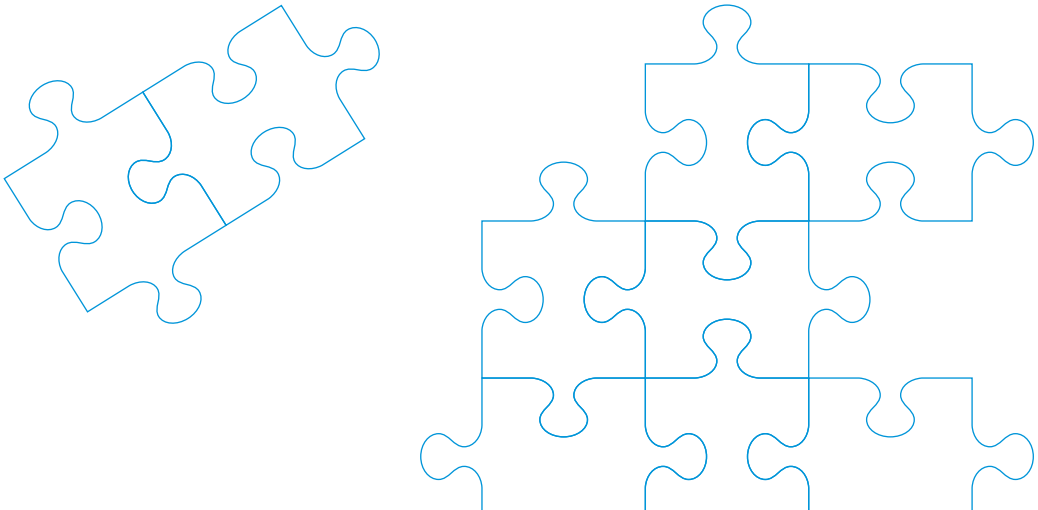
- *The Strategic Leading Group* (SLG) at the national level in the Police Directorate of the Ministry of Interior is chaired by the Serbian National Police Director. Its main functions and responsibilities fall under the following categories: tasking or requesting a strategic assessment for public safety and other national criminal intelligence products; strategic planning, including decision-making and resource allocation, based on the strategic assessment and other concrete criminal intelligence products; and monitoring and verifying the implementation of the strategic plans.

- *The Operational Leading Group Criminal Police* at the national level (OLG CPG) is chaired by the Head of Criminal Police, with the following main functions: developing an Annual Operational Plan at the national level for the prevention and suppression of crime, based on strategic plans from the SLG; allocating resources for key objectives of the Annual Operational Plan; and tasking/requesting and decision-making based on concrete criminal intelligence products in areas of serious and organized crime.

- *Operational Leading Groups* at the regional level (OLG RPD) are chaired by each of the 27 Heads of the Regional Police Directorates, with the following main functions: operational planning at the regional level for prevention and suppression of crime, based on strategic plans from the SLG; tasking and co-ordination of operational activities at the RPD level; decision-making based on concrete criminal intelligence product at the regional level; and evaluation of completed regional police tasks, operations and investigations.

- *Operational Leading Groups* at the local/station level (ORG PS) is made up of police station management and chaired by Station Commanders. The ORG PS have the following main functions: operational planning on local/station level for prevention and suppression of crime, based on strategic plans from the SLG, OLG RPD Annual Operational Plan and criminal intelligence products; decision-making, tasking and co-ordination at the local/station level of operational activities, including investigation.

In addition to being a model for managing operational police work on the basis of criminal intelligence, the ILP model is also intended to embed quality management. In the Serbian ILP Handbook, the term "quality" is emphasized in connection with the ILP process, human resources, training, criminal-intelligence products, standards and quality criteria, as well as in connection with the relationship between the strategic and operational leading and steering groups, on the one hand, and the analysis service, on the other hand. All this highlights that quality is a recognized as a significant feature of the ILP model.



8.2.5 Montenegro: Serious and organized crime threat assessments

Following recommendations set forth in the Montenegrin Serious and Organized Crime Threat Assessment (SOCTA MNE), a relevant law enforcement authority decides on a list of a number of national, inter-agency priorities to fight serious and organized crime. These priorities are reflected in the setting of specific operational and investigative priority tasks and inter-agency co-ordination.

As Figure 8.8 explains, SOCTA MNE covers the period of four years and is developed by an inter-agency team composed of representatives of the Montenegrin intelligence and the security sector.

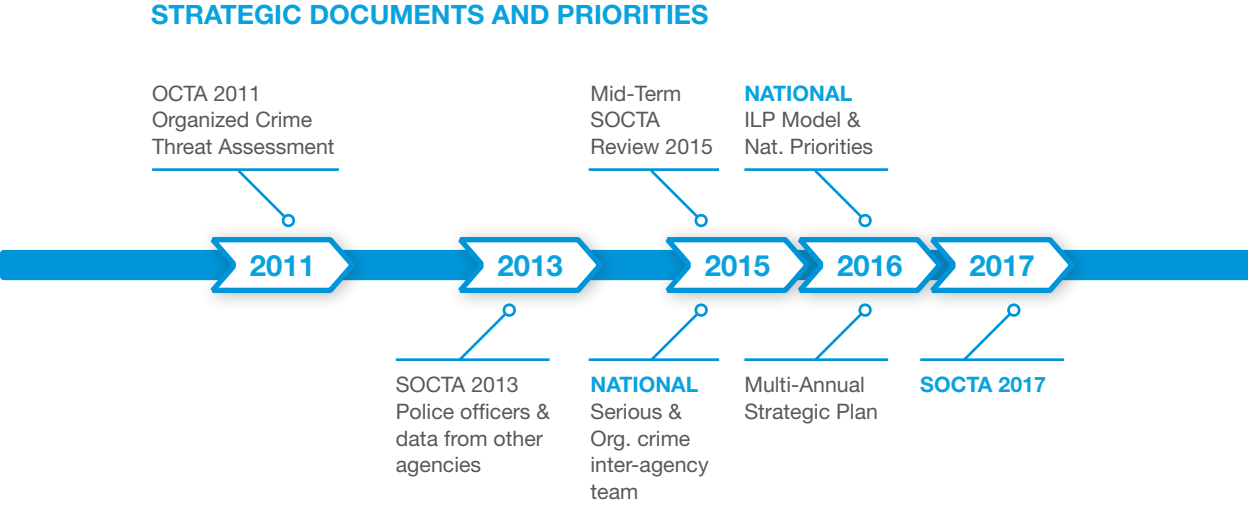


Figure 8.8 **SOCTA developments and strategic planning in Montenegro**

SOCTA MNE 2013-2017 priorities include the following areas:

- *serious crimes against life and body* generated as a consequence of a conflicts between organized criminal groups;
- *terrorism and religious extremism*,[77] primarily related to the participation of Montenegrin citizens in foreign armed forces as well as the strengthening of religious extremism in the area of the Balkan Peninsula;
- *high-level corruption* committed by persons who have the status of public officials;
- *drug trafficking, which is a dominant* criminal activity of the largest number of organized criminal groups;

77 The OSCE terminology is "violent extremism".

- *loan sharking*, which is recognized as a particular problem that results in the commission of other serious criminal offenses;
- *illegal migration and trafficking in human beings*, which is characterized by abuse of the asylum procedure as well as labor and sexual exploitation; and
- *money laundering and financial investigations*, which is recognized as being effective means in the fight against organized crime.

The National Interagency Operational Team[78] is a working group for the fight against serious and organized crime, established in 2015. The Operational Team is a multi-agency body, consisting of representatives of the following agencies:

- Ministry of Justice
- Police
- National Security Agency
- Customs
- Department of Public Revenues
- Administration for Prevention of Money Laundering and Terrorist Financing.

The Interagency Operational Team has the following tasks:

- proposing national priorities in the fight against serious and organized crime;
- proposing strategic goals and multi-annual strategic plans in the fight against serious and organized crime;
- proposing a National Intelligence Model for establishing priorities, managing and assigning tasks in addressing serious and organized crime based on the SOCTA MNE;
- adopting and implementing annual operational plans in the fight against serious and organised crime, based on established strategic priorities;
- ensuring interagency co-operation in carrying out particular activities on the operational level in the fight against serious and organized crime;
- considering measures for efficient implementation of the National Intelligence Model in establishing priorities, managing and assigning tasks based on the SOCTA MNE;
- submitting quarterly reports on its work to the Bureau for Operational Coordination; and
- performing other tasks in order to direct activities in the fight against serious and organized crime.

Montenegro has slightly modified the Canadian RCMP Sleipnir assessment methodology, which is being used in assessing threats from identified organized criminal groups and for comparing threat rankings between groups as well as to identify intelligence gaps that need to be filled. The modified Montenegrin version of the Sleipnir model includes 14 threat criteria subject to assessment, as presented in Table 8.3.

78 Official Gazette of Montenegro. "Law on Basis of the Intelligence and Security Sector of Montenegro". *No. 28/14:* Art 17.

Table 8.3 **The Montenegrin version of the Sleipnir assessment tool**

Group ID N = National R = Regional L = Local	Threat score	Corruption	Violence	Legitimate businesses	Money laundering	Cooperation with criminal groups	Protection of Leaders	Monopoly	Territory of action	Countermeasures	Diversity (crime)	Discipline/order	Cohesion	Size	Expertise
N-RV01-00	230.3														
N-RA03-00	226.0														
N-BK02-06	215.4														
N-BK06-09	212.1														
R-BS01-92	209.3														
R-BS01-90	206.8														
R-NI04-08	202.9														
R-NI01-95	193.5														
R-HI02-08	191.7														
R-BK01-06	189.1														
R-HI01-08	184.1														
R-UR07-09	183.7														
L-UK02-05	180.2														
L-IA01-97	177.9														
L-PG02-00	174.2														
L-BS06-11	172.7														
L-BS04-00	172.1														
L-BS08-00	171.2														
L-HI04-10	161.1														
L-HI03-10	143.2														

Threat	High	Medium	Unknown	Low	Nil
The value of the attribute in the matrix					

8.3 ILP and community policing

Community policing focuses on collective problem solving, crime prevention and the building of trust between the police and the communities they serve. Community policing practices and principles help to establish and strengthen police-public partnerships, where the police, governmental agencies and local communities actively co-operate to solve problems together and address community grievances.[79] The community policing movement is anchored in the notion that greater community engagement will improve police operations and organizational performance, as well as police legitimacy in the eyes of the public.

The specific focus of community policing is increasing and improving relations between the community and the police, and involves a fundamental shift toward identifying local crime and disorder concerns jointly with the police, and where possible, addressing and resolving them jointly. It is built on the belief that a more co-ordinated and collaborative approach can address current problems as well as prevent future ones. This approach also involves working in a more multi-disciplinary manner and with the possibility of several other partners including municipal governments, other government agencies or departments, or community associations, being involved in a programme.

Community policing can also lead to better and more reliable communications with and from the public. Although community policing officers should not be tasked to gather intelligence, increased trust can represent an invaluable source of community information and awareness for the police. This has the potential to become valuable information for the police to plan and target their anti-crime and terrorism operations more effectively, and thus, community policing and ILP directly support one another.

Community policing has sought to broaden policing mandates from a narrow crime fighting and investigation focus to one that engages more directly with the community in order to generate community views and concerns often on a wide range of issues: include fear of crime, crime prevention, physical disorder, and other social and neighbourhood problems. The core principles reflected in community policing include a more service-oriented approach built around the themes of 'visibility', 'accessibility' and 'familiarity', with a particular focus on collective problem solving.[80] It also provides the means whereby the police are able to engage more effectively with the public, and identify and resolve those problems that are the public's priorities.[81]

According to key principles of community policing, the police should:

- *engage*, mobilize and partner with communities;
- *listen* to communities' concerns;

---

79 OSCE (2008a: 89).

80 Innes, Martin. Why 'soft' policing is hard: on the curious development of reassurance policing, how it became neighbourhood policing and what this signifies about the politics of police reform. *Journal of community applied social psychology*, Vol. 15, No. 3 (2005: 156–169); and Quinton, Paul and Morris, Julia. "Neighbourhood policing: the impact of piloting and early nation implementation.", (Home Office Online Report, 01/2008) [http://webarchive.nationalarchives.gov.uk/20110314171826/http://rds.homeoffice.gov.uk/rds/pdfs08/rdsolr0108.pdf] Accessed 2 June 2017.

81 Bullock (2013: 126-127).

- *be involved* in joint problem solving with the community;
- *be visible* and *accessible* to the public;
- *know* the public and be known by them;
- *respond* to communities' needs;
- *respect* and *protect* the rights of all community members; and
- *be accountable* for their actions and their outcome of these actions.[82]

As discussed in Chapter 3, ILP was developed to challenge the dominant and traditional reactive, response-based policing model. ILP is a top-down managerial decision-making framework and approach, and has implications for both how policing is organized and how it operates. On the organizational side, unlike community policing, which gives individual police officers substantial latitude in developing their relations with local communities, ILP is necessarily more centralized. Systematic gathering and analysis of data and information provide the basis for informed managerial decisions.

ILP and community policing are complementary and mutually supportive approaches that still have some distinct characteristics with regard to their orientation, hierarchical focus and the decision-making actors, described in Table 8.4.

Table 8.4 **Comparison of key dimensions of community policing and intelligence-led policing**

	COMMUNITY POLICING	INTELLIGENCE-LED POLICING
Orientation?	Local communities and neighbourhoods	Criminal groups, prolific and serious offenders, counter-terrorism and VERLT
Hierarchical focus?	Bottom-up	Top-down
Who determines priorities?	Community concerns/ demands	Policymakers and police management from criminal intelligence analysis

The criteria for success and the expected benefits of both approaches are similar, aiming for:
- increased police effectiveness based on increased information flow;
- increased community safety and security resulting in increased public satisfaction.

Gathering of intelligence should never be the primary objective of community policing but can be a by-product of effective community policing. Complementing and supporting ILP, community policing can facilitate the sharing of information between the public and the police by building public trust and confidence in the police, and increasing the number of opportunities for interaction between the public and the police.

82 OSCE, ODIHR/TNTD (2014: 76).

In turn, the tasking and co-ordinating efforts of ILP may strengthen the effects of community policing through the information analysis processes and through its hierarchical structures. The more positive nature of the police-citizen relationship now promotes a more continuous and reliable transfer of information from one to the other.

"Community policing has developed skills in many law enforcement officers that directly support new ILP responsibilities: The scientific approach to problem solving, environmental scanning, effective communications with the public, fear reduction, and community mobilization to deal with problems are among the important attributes community policing brings to this challenge."[83]

Thus, there is potential for community-policing efforts to serve as a gateway of locally based information to prevent and target all forms of crime, including violent extremism and terrorism (see sub-chapter 8.4). At the same time, ILP can help community officers to identify, prioritize and address issues of public concern more effectively.

> "Neighbourhood policing should act to generate information and that information should be incorporated into and help fuel the National Intelligence Model process. Guidance has drawn attention to how information may be generated from communities in different ways. This may include the observations of members of the public; information obtained by officers in the course of their duties within neighbourhoods; and information derived from other public sector workers such as teachers and doctors. Doing so has been assumed to increase knowledge of risk and vulnerability; improve opportunities for community engagement; and increase community confidence. Additionally, as we have seen, one aim of neighbourhood policing has been to proactively identify and tackle crime problems which are priorities for local communities. Police officers should view these priorities as 'intelligence' and incorporate them into National Intelligence Model systems."
>
> **– Bullock (2013: 128-131).**

A more local focus and approach also supports the prevention of terrorism and countering VERLT, where communities have emerged as a key point of focus in the formulation and implementation of counterterrorism policies. This is based on the idea that terrorism and

83 Carter (2009: 86-87).

VERLT are threats to community security, not just state security, and that communities are therefore also stakeholders and partners in counter-terrorism. Countering terrorism, and in particular countering VERLT, also requires a multi-disciplinary and co-ordinated approach, involving a broad range of public authorities beyond the security and criminal justice sectors. By engaging with a broader number of people and engaging them on a diverse range of issues not limited to empowerment against terrorism, the state can diminish the risk of stigmatizing particular communities.[84]

8.4 ILP in preventing and countering terrorism and VERLT

Good policing is good terrorism prevention; thus, professional policing is instrumental in uncovering intelligence associated with both terrorist activities and conventional crimes. Encouraging this perspective enables local police departments to involve line officers more actively and to reinforce the fact that enforcement, crime prevention, and terrorism prevention are interrelated. This approach helps to balance the current emphasis on anti-terrorism activities with traditional anti-crime efforts. Many line officers want to define their role in the fight against terrorism. ILP can help clarify their contributions in this regard.[85]

With managerial guidance and proper training, ILP practice can provide all law enforcement officers with a clear vision for their role in preventing and countering terrorism and VERLT. If ILP structural and procedural channels are in place and well-functioning, gathering and forwarding information and suspicions become an integral part of day-to-day duties of all law enforcement, including general policing, border management and customs services.

Policies and programmes aiming to build contacts and trust with local communities, including businesses, religious communities, youth and education leaders, and cultural centres, may help in preventing and addressing violent extremism and terrorism. Thus, some countries have redefined community policing within an ILP framework for counterterrorism purposes, putting in place structures and processes, within national legal frameworks, for obtaining and analysing information from the public and the local levels.[86]

As mentioned in sub-chapter 8.3, it must be clearly understood by the police and the communities that community policing not only involves the gathering of intelligence, but also safeguarding the communities' needs. Still, the main task of community policing remains the building and maintenance of police-public partnerships, based on mutual respect and trust.[87]

84 OSCE, ODIHR/TNTD (2014: 74).

85 Peterson (2005: 15-16).

86 Ratcliffe (2016: 115).

87 OSCE ODIHR/TNTD (2014: 179).

> "There is one area where community policing could be the only viable option to gather useful information from the community. In a counter-terrorism scenario, numerous commentators have argued that community policing will be more effective at gathering local information and potential intelligence, and more in line with public expectations of police in a democratic nation, than covert tactics and other intelligence techniques." **– Innes (2006: 229).**

Where there is a shared understanding by both police and communities that the aim of the police and partner agencies in countering VERLT is to first and foremost protect the vulnerable from radicalizing influences, trust can be more easily built. Concerns of spying and targeting of communities by the police can be largely alleviated when communities understand that the police's role is to protect them and when VERLT is explained in the context of safeguarding the community, for example, preventing child sexual exploitation or human trafficking. Certainly, experience from the United Kingdom has shown that suspicion of its prevent strategy and policy activity can be mitigated when the police, central and local government agencies work together to deliver a consistent message that the prevent strategy is simply and fundamentally aimed at protecting the vulnerable from radicalizers, irrespective of their community of origin.

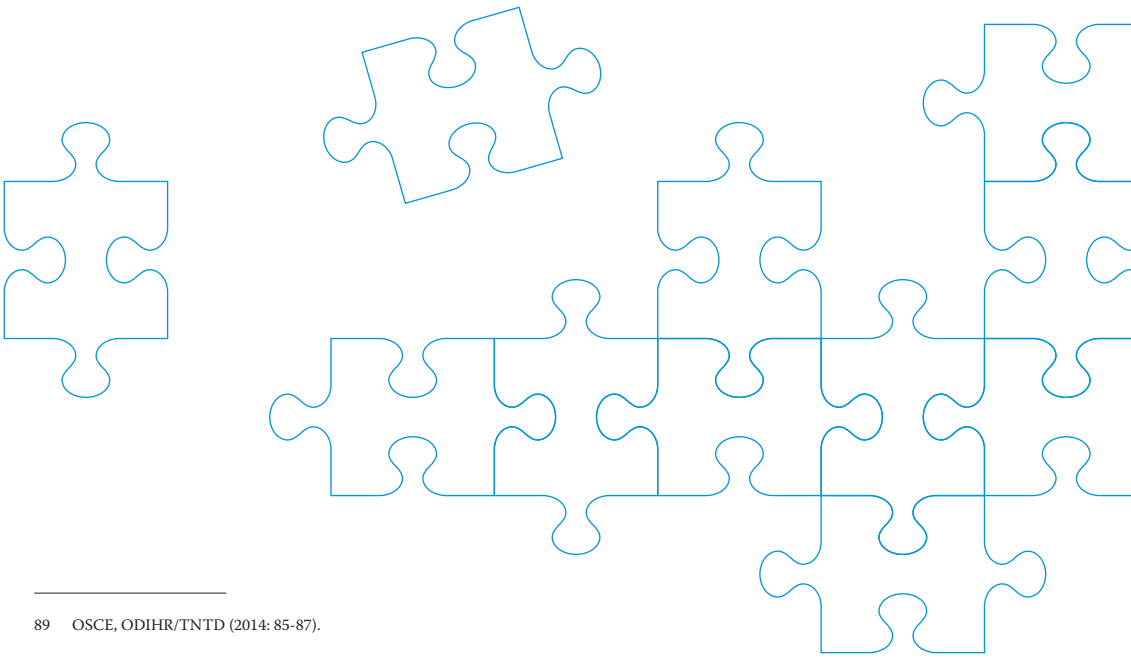
To facilitate this important role of community policing, community policing officers must be trained on where to look for and how to identify signs of terrorism planning or VERLT, and how to forward the information in line with national SOPs through relevant channels to a centralized analysis entity. Officers should also undertake specialized training on human rights in order to perform such tasks in full respect of human rights standards.[88] It is also imperative that local officers who forward such information receive feedback from their efforts in this regard.

In order to support the central role of community policing in building the police-public partnership and crime prevention at all levels, including serious crime and suspected terrorism-related activity, or preventing and countering VERLT, some countries have established specially trained officers in VERLT, deployed in addition to and in support of the local community policing officers. Decisions on the locality of this long-term resource deployment are based on intelligence analysis providing an assessment of risk and threat from VERLT on a geographical basis. Within a predefined structure and based on formal decisions rooted in national legislation, these officers engage with communities as community policing officers would, but with the specific and explicit purpose of overtly working with communities and civic society groups to build trust and minimize risk and threat associated with VERLT. Like community policing officers, these specialist officers submit information for evaluation and assessment through formal communication channels to a central analysis function or insert it direct into national databases. The emphasis of this specialist role is, as always, to work in the

88 OSCE, ODIHR/TNTD (2014: 106-107).

community and with communities and to engage all stakeholders in preventing VERLT; it is not about spying on these communities.

As outlined in Chapter 7, ILP relies on well-functioning organizational structures and communication systems that can facilitate two-way information flow between communities, community policing officers and other local sources, and a central analysis entity. Again, it must be stressed that the main objective of community policing is not to spy on communities, but rather to establish positive connections and increase trust between the police and the public to enable the flow of information and intelligence. Community engagement in the context of VERLT needs to build on functioning police-community relations and community support, which cannot be assumed; it must be won. Trusting relations between the police and various sections of the community need to be developed long before sensitive issues such as VERLT can be addressed in joint efforts.[89] Where community policing officers have established trust and healthy communication channels with their local communities, they may be the strongest or even the only source of information coming from the community that can identify the driving factors of terrorist radicalization, which could lead to the prevention of terrorist incidents or identify the individuals that may be vulnerable to terrorist radicalization.



89 OSCE, ODIHR/TNTD (2014: 85-87).

References

Australian Criminal Intelligence Management Strategy 2012-2015 (Commonwealth of Australia, 2012). [www.afp.gov.au/sites/default/files/PDF/ACIM-strategy-2012-15.pdf] Accessed 27 April 2017.

Bell, Peter and Congram, Mitchell. "Intelligence-Led Policing (ILP) as a Strategic Planning Resource in the Fight against Transnational Organized Crime (TOC)." *International Journal of Business and Commerce, Vol. 2, No. 12* (2013): 15-28. [www98.griffith.edu.au/dspace/bitstream/handle/10072/64598/98685_1.pdf;sequence=1] Accessed 5 April 2017.

Bullock, Karen, "Community, intelligence-led policing and crime control." *Policing and Society, Vol. 23, No. 2* (2013): 125-144.

Carter, David L., *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*. 2nd Edition (Washington, DC: U.S Department of Justice, 2009).

Conference on Security and Co-operation in Europe, *Final Act* (Helsinki: 1975). [www.osce.org/mc/39501?download=true] Accessed 6 April 2017.

Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR), (4 November 1950). [www.echr.coe.int/pages/home.aspx?p=basictexts] Accessed 28 April 2017.

Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, European Treaty Series, No. 108 (Strasbourg: 28 January 1981). [conventions.coe.int/Treaty/en/Treaties/Html/108.htm] Accessed 27 April 2017.

Council of Europe, *The European Code of Police Ethics* (Strasbourg: Council of Europe Publishing, March 2002). [www.bak.gv.at/cms/BAK_dt/download/downloads/files/Verhaltenskodex/CoE_FRA_RPT_2687_EN_500.pdf] Accessed 27 April 2017.

European Court of Human Rights. Case of Shimovolos v. Russia. Application no. 30194/09 (Strasbourg: 21 June 2011). [hudoc.echr.coe.int/eng#{"appno":["30194/09"],"itemid":["001-105217"]}] Accessed 28 April 2017.

European Court of Human Rights. Case of Roman Zakharov v. Russia. Application no. 47143/06 (Strasbourg: 4 December 2015). [lovdata.no/static/EMDN/emd-2006-047143.pdf] Accessed 28 April 2017.

European Court of Human Rights. Case of Szabo and Vissy v. Hungary. Application no. 37138/14 (Strasbourg: 12 January 2016). [www.statewatch.org/news/2016/jan/echr-case-SZAB-%20AND-VISSY-v-%20HUNGARY.pdf] Accessed 28 April 2017.

Council of the European Union. "Council conclusions on intelligence-led policing and the development of the Organized Crime Threat Assessment (OCTA)." Doc. 10180/4/05, REV 4, (Brussels: 3 October 2005). [register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010180%20 2005%20REV%204] Accessed 27 April 2017.

Council of the European Union. "Council Framework Decision of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union." *Official Journal of the European Union* (2006/960/JHA, 18 December 2006). [eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri=CELEX:32006F0960&from=EN] Accessed 27 April 2017.

Council of the European Union. "Council conclusions on the creation and implementation of a EU policy cycle for organised and serious international crime." 3043rd Justice and Home Affairs Council Meeting, (Brussels: 8 and 9 November 2010). [https://www.consilium. europa.eu/uedocs/cms_data/docs/pressdata/en/jha/117583.pdf] Accessed 6 April 2017.

Council of the European Union. "Serious and Organised Crime Threat Assessment (SOCTA) – Methodology." Doc. 9992/2/12, REV 2, COSI 28, (Brussels: 19 June 2012). [www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/p24_ soctamethodology_/p24_soctamethodology_en.pdf] Accessed 6 April 2017.

Council of the European Union. "EMPACT Terms of Reference." Doc. 14518/12, COSI 82, *(Brussels: 3 October 2012).* [www.statewatch.org/news/2012/oct/eu-council-cosi-empact-tor-14518-12.pdf] Accessed 6 April 2017.

Council of the European Union. "Council conclusions on setting the EU's priorities for the fight against serious and organised crime between 2014-2017." Justice and Home Affairs Council meeting, (Luxembourg: 6 and 7 June 2013). [www.consilium.europa.eu/uedocs/ cms_data/docs/pressdata/en/jha/137401.pdf] Accessed 6 April 2017.

Council of the European Union, *The EU Policy Cycle to tackle organized and serious international crime* (Brussels: 2014).

Council of the European Union. "Serious and Organised Crime Threat Assessment 2017 – Revised methodology." Doc. 14913/15, CRIMORG 128, Brussels: 11 December 2015. [www.statewatch.org/news/2015/dec/eu-council-socta-2017-methodology-14913-15.pdf] Accessed 6 April 2017.

Criminal Intelligence Service Canada, *Integrated Threat Assessment Methodology, Version 1.0* (Ottawa, Ontario: Criminal Intelligence Service Canada, 2007).

Eck, John E., Clarke, Ronald V. and Petrossian, G., *Intelligence Analysis for Problem Solvers* (Washington, DC: U.S. Department of State, Community Oriented Policing Services, 2013).

European External Action Service, *Handbook on Intelligence Led Policing (ILP) for civilian CSDP Missions* (Civilian Planning and Conduct Capability, Belgium Ministry of Foreign Affairs, Belgium Federal Police, 2013).

Europol, *EU Policy Cycle SOCTA Empact* (Europol, 2010). [https://www.europol.europa.eu/publications-documents/eu-policy-cycle-socta-empact] Accessed 27 April 2017.

Europol, *SOCTA 2013 – EU Serious and Organised Crime Threat Assessment* (The Hague: European Police Office, 2013). [https://www.europol.europa.eu/activities-services/main-reports/eu-serious-and-organised-crime-threat-assessment-socta-2013] Accessed 27 April 2017.

Europol, *Exploring Tomorrow's Organized Crime* (The Hague: European Police Office, 2015). [https://www.europol.europa.eu/publications-documents/exploring-tomorrow's-organised-crime] Accessed 27 April 2017.

Europol, *SOCTA 2017 – European Union Serious and Organised Crime Threat Assessment 2017* (The Hague: European Police Office, 2017) [https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017] Accessed 28 April 2017.

Flood, B. and Gaspar, R. "Strategic aspects of the UK National Intelligence Model." In: "The path to enlightenment: Limiting costs and maximizing returns from intelligence-led policy and practice in public policing." *Policing: A Journal of Policy and Practice*, ed. Adrian James (Oxford University Press, 2017).

Geneva Centre for Security, Development and Rule of Law (DCAF), *Criminal Intelligence Manual* (Ljubljana: Institute DCAF Ljubljana, 2014). *[dcaf-ljubljana.si/116]* Accessed 27 April 2017.

Innes, Martin. "Why 'soft' policing is hard: on the curious development of reassurance policing, how it became neighbourhood policing and what this signifies about the politics of police reform." *Journal of community applied social psychology,* Vol. 15, No. 3 (2005: 156–169).

Innes, Martin. "Policing uncertainty: Countering terror through community intelligence and democratic policing". *The Annals of the American Academy of Political and Social Science, Vol. 605, No. 1* (2006): 222-241.

International Association of Chiefs of Police. "Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels." IACP Intelligence Summit, Alexandria, VA (2002).

INTERPOL. "Criminal Intelligence Analysis." *Fact Sheet* (2014). [https://www.interpol.int/INTERPOL-expertise/Criminal-Intelligence-analysis] Accessed 27 April 2017.

James, Adrian D.; Phythian, Mark; Richards, Julian and Wadie, Fiona C., '*What works?' in police intelligence practice*? (The National Police Chiefs Council, 2016).

James, Adrian. "The path to enlightenment: Limiting costs and maximizing returns from intelligence-led policy and practice in public policing." *Policing: A Journal of Policy and Practice* (Oxford University Press, 2017).

Karn, Jacqui, *Policing and Crime Reduction: The evidence and its implications for practice* (London: The Police Foundation, 2013).

Kelling, George L., and Bratton, William J. "Policing terrorism." *Civic Bulletin 43, No. 12* (2006).

Kosovo Police, *Handbook Intelligence led policing* (Pristina: 2016). [Unpublished].[90]

Murdoch, Jim and Roche, Ralph, *The European Convention on Human Rights and Policing: A Handbook for police officers and other law enforcement officials* (Strasbourg: European Union/Council of Europe, 2013).

Ministry of Interior of the Republic of Serbia, *Handbook on the police intelligence model* (2016). [www.mup.gov.rs] Accessed 28 April 2017.

Ministry of Interior of the Republic of Serbia. "Decree on the Promulgation of the Law on Police." PR No. 1, (Belgrade: 28 January 2016). [arhiva.mup.gov.rs/cms_eng/home.nsf/Law-on-Police-adopted-01-03-2016.pdf] Accessed 03 May 2017

National Criminal Intelligence Service (NCIS), *The National Intelligence Model* (NCIS Corporate Communications, 2000). [www.intelligenceanalysis.net/National%20 Intelligence%20Model.pdf] Accessed 27 April 2017.

National Policing Improvement Agency, *Practice Advice on Analysis* (Association of Chief Police Officers, 2008). [library.college.police.uk/docs/npia/practice_advice_on_analysis_ interactive.pdf] Accessed 27 April 2017.

O'Neill, Maria, Swinton, Ken and Winter, Aaron, *New Challenges for the EU Internal Security Strategy* (Newcastle, UK: Cambridge Scholars Publishing, 2013).

Official Gazette of Montenegro "Law on Basis of the Intelligence and Security Sector of Montenegro.", *No. 28/14*. [www.sluzbenilist.me/PravniAktDetalji.aspx?tag=%7B65668A19-BB7B-4029-BDC4-1D46FE9208E2%7D] Accessed 03 May 2017.

90 All references to Kosovo, whether to the territory, institutions or population, in this text should be understood in full compliance with United Nations Security Council Resolution 1244.

OSCE, *Concluding Document of the Vienna Meeting 1986 of Representatives of the Participating States of the Conference on Security and Co-operation in Europe, held on the basis of the provisions of the Final Act relating to the follow-up to the Conference* (Vienna: 1989). [www.osce.org/mc/40881?download=true] Accessed 27 April 2017.

OSCE, *Document of the Moscow Meeting of the Conference on the Human Dimension of the CSCE* (Moscow, 3 October 1991). [www.osce.org/odihr/elections/14310] Accessed 18 April 2017.

OSCE, *Good Practices in Building Police-Public Partnerships by the Senior Police Adviser to the OSCE Secretary General* (Vienna: OSCE, 2008a). [www.osce.org/spmu/32547?download=true] Accessed 28 April 2017.

OSCE, *Guidebook on democratic policing, by the Senior Police Adviser to the OSCE Secretary General,* 2nd Edition (Vienna: OSCE, 2008b). [www.osce.org/spmu/23804] Accessed 6 April 2017.

OSCE, *Human rights in counter-terrorism investigations – A Practical Manual for Law Enforcement Officers* (Warsaw: Office for Democratic Institutions and Human Rights (ODIHR) and Transnational Threats Department (TNTD), 2013). [www.osce.org/odihr/108930?download=true] Accessed 6 April 2017.

OSCE, *Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Community-Policing Approach* (Vienna: ODIHR and TNTD, 2014). [www.osce.org/atu/111438] Accessed 27 April 2017.

OSCE. "Assessments of OSCE Field Operations' engagement in national intelligence-led policing programmes in OSCE participating States." Vienna: OSCE, Transnational Threats Department/Strategic Police Matters Unit (TNTD/SPMU), 17 February 2016. [Unpublished/internal].

OSCE. "Status of Intelligence-Led Policing Concepts in International Security and Law Enforcement Organizations". *Interoffice Memorandum* (Vienna: OSCE, 26 April 2016). [Unpublished/internal].

OSCE Chiefs of Police Meeting, *Brussels Statement* (24 November 2006). [www.osce.org/spmu/23260?download=true] Accessed 6 April 2017.

OSCE Ministerial Council, Ministerial Statement. "Sofia Ministerial Statement on Preventing and Combating Terrorism" (Sofia: MC(12).JOUR/2, 7 December 2004). [www.osce.org/mc/38760?download=true] Accessed 6 April 2017.

OSCE Ministerial Council, Ministerial Statement. "Brussels Ministerial Statement on Supporting and Promoting the International Legal Framework against Terrorism" (Brussels: MC.DOC/5/06, 5 December 2006). [www.osce.org/mc/23029?download=true] Accessed 6 April 2017.

OSCE Ministerial Council, Decision No. 5/06. "Organized Crime" (Brussels: MC.DEC/5/06, 5 December 2006). [www.osce.org/mc/23060?download=true] Accessed 6 April 2017.

OSCE Permanent Council, Decision No. 1049. "OSCE Strategic Framework for Police-Related Activities" (Vienna: PC.DEC/1049, 26 July 2012). [www.osce.org/pc/92559?download=true] Accessed 6 April 2017.

Pajevic, Maid. "Application of the Theory of Criminal Intelligence in Police Work". *E-Journal of Police Studies (Ijps), Internacionalna asocijacija policijskih akademija (INTERPA)* (2014).

Parliamentary Joint Committee on Law Enforcement, *Inquiry into the gathering and use of criminal intelligence* (Canberra Parliamentary Joint Committee on Law Enforcement, Commonwealth of Australia, 2013).

Peterson, Marilyn, *Intelligence-Led Policing: The New Intelligence Architecture* (Washington, DC: U.S. Department of Justice, Bureau of Justice Assistance, 2005).

Quinton, P. and Morris, J. "Neighbourhood policing: The impact of piloting and early national implementation." (Home Office Online Report, 01/2008) [http://webarchive.nationalarchives.gov.uk/20110314171826/http://rds.homeoffice.gov.uk/rds/pdfs08/rdsolr0108.pdf] Accessed 2 June 2017.

Ratcliffe, Jerry H., *Intelligence-Led Policing* (Cullompton, UK: Willan Publishing, 2008).

Ratcliffe, Jerry H., Strang, Steven and Taylor, Ralph. "Assessing the success factors of organized crime groups". *Policing: an International Journal of Police Strategies & Management, Vol. 37, No. 1* (2014: 206-227).

Ratcliffe, Jerry H., *Intelligence-Led Policing*, 2nd Edition (London/New York: Routledge, 2016).

Renard, Thomas. "Counterterrorism in Belgium: Key Challenges and Policy Options." *Egmont Paper 89* (Brussels: Egmont Institute, 2016).

Royal Canadian Mounted Police Criminal Intelligence. "Sleipnir Version 2.0, Organized Crime Groups Capability Measurement Matrix.", (Ottawa: RCMP, 2011). [www.yumpu.com/en/document/view/51586046/sleipnir-version-20-organized-crime-groups-capability-] Accessed 27 April 2017.

Stevens, John, "Intelligence-Led Policing". Paper presented at the Institute for Human Rights and Criminal Justice Studies international conference, Durban, 3-7 December 2001.

United Nations Department of Peacekeeping Operations (UNDPKO). "Guidelines on Police Operations in United Nations Peacekeeping Operations and Special Political Missions." Ref. 2015.15, 01 January 2016. [www.un.org/en/peacekeeping/sites/police/documents/Guidelines_Operations.pdf] Accessed 27 April 2017.

United Nations General Assembly. "International Covenant on Civil and Political Rights (ICCPR)." *No. 14668, United Nations Treaty Series, Vol. 999* (New York: 16 December 1966). [www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx] Accessed 27 April 2017.

United Nations General Assembly, Resolution 34, "Code of Conduct for Law Enforcement Officials." A/RES/34/169, 17 December 1979. [www.ohchr.org/EN/ProfessionalInterest/Pages/LawEnforcementOfficials.aspx] Accessed 28 April 2017.

United Nations General Assembly, Resolution 45/95, "Guidelines for the regulation of computerized personal data files." A/RES/45/95, 14 December 1990. [www.un.org/documents/ga/res/45/a45r095.htm] Accessed 27 April 2017.

United Nations General Assembly. "Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin." Report to the UN Human Rights Council, 4 February 2009, A/HRC/10/3. [www.ohchr.org/EN/Issues/Terrorism/Pages/Annual.aspx] Accessed 27 April 2017.

United Nations General Assembly. "Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin. Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight." Report to the UN Human Rights Council, 17 May 2010, A/HRC/14/46. [www.ohchr.org/EN/Issues/Terrorism/Pages/Annual.aspx] Accessed 28 April 2017.

United Nations General Assembly. "Special Rapporteur on the rights to freedom of peaceful assembly and of association Maina Kiai, Addendum, Mission to the United Kingdom of Great Britain and Northern Ireland." Report to the UN Human Rights Council, 17 June 2013, A/HRC/23/39/Add.1. [www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A-HRC-23-39-Add1_en.pdf] Accessed 28 April 2017.

United Nations General Assembly. "Special Rapporteur on torture and other cruel, inhuman or degrading treatment or punishment, Juan E. Méndez." Report to the UN Human Rights Council, 10 April 2014, A/HRC/25/60. [ap.ohchr.org/documents/dpage_e.aspx?m=103] Accessed 28 April 2017.

United Nations General Assembly. "Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson." Annual Report to the UN General Assembly, 23 September 2014, A/69/397. [www.ohchr.org/EN/Issues/Terrorism/Pages/Annual.aspx] Accessed 28 April 2017.

United Nations General Assembly. "Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson." Report to the UN Human Rights Council, 16 June 2015, A/HRC/29/51. [ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/29/51] Accessed 28 April 2017.

United Nations General Assembly. "Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism." Report to the UN Human Rights Council, 21 February 2017, A/HRC/34/61. [www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/_layouts/15/WopiFrame.aspx?sourcedoc=/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A_HRC_34_61_EN.docx&action=default&DefaultItemOpen=1] Accessed 28 April 2017.

United Nations Human Rights Committee, *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation* (8 April 1988). [www.refworld.org/docid/453883f922.html] Accessed 28 April 2017.

United Nations Office on Drugs and Crime (UNODC), United Nations Convention against Corruption (Vienna: United Nations Publication, 2004). [www.unodc.org/unodc/en/corruption/tools_and_publications/UN-convention-against-corruption.html] Accessed 27 April 2017.

UNODC, *United Nations Convention Against Transnational Organized Crime and the Protocols Thereto* (Vienna: United Nations Publication, 2004). [www.unodc.org/unodc/treaties/CTOC/#Fulltext] Accessed 27 April 2017.

UNODC, *Policing – Police Information and Intelligence Systems. Criminal Justice Assessment Toolkit* (Vienna: United Nations Publication, 2006). [www.unodc.org/documents/justice-and-prison-reform/cjat_eng/4_Police_Information_Intelligence_Systems.pdf] Accessed 27 April 2017.

UNODC, *Current Practices in Electronic Surveillance in the Investigation of serious and organized crime* (Vienna: United Nations Publication, 2009). [www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf] Accessed 27 April 2017.

UNODC, *Criminal Intelligence – Manual for Front-line Law Enforcement* (Vienna: United Nations Publication, 2010a). [www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Front_Line_Law_Enforcement.pdf] Accessed 27 April 2017.

UNODC, *Guidance on the preparation and use of serious and organized crime threat assessments. The SOCTA Handbook* (Vienna: United Nations Publication, 2010b). [www.unodc.org/documents/organized-crime/Law-Enforcement/SOCTA_Handbook.pdf] Accessed 27 April 2017.

UNODC, *Criminal Intelligence – Manual for Analysts* (Vienna: United Nations Publication, 2011a). [www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf] Accessed 27 April 2017.

UNODC, *Criminal Intelligence – Manual for Managers* (Vienna: United Nations Publication, 2011b). [www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Managers.pdf] Accessed 27 April 2017.

United States Department of Justice, *Reducing Crime Through Intelligence-Led Policing* (Washington, DC: U.S Department of Justice, Bureau of Justice Assistance, 2009).

United States Department of Justice, *Law Enforcement Analytic Standards.* 2nd Edition (Washington, DC: U.S Department of Justice, Bureau of Justice Assistance, 2012).

Weisburd, David and Eck, John E. "What can the police do to reduce crime, disorder and fear?" *Annals of the American Academy of Social and Political Sciences, Vol. 593* (2004): 42–65.

Wells, Ronald, "Intelligence-Led Policing: a new paradigm in law enforcement." *Public Agency Training Council (PATC), E-Newsletter* (2009). [www.patc.com/weeklyarticles/intelligence_policing.shtml] Accessed 6 April 2017.

Websites

Center for Problem-Oriented Policing
www.popcenter.org/about/?p=whatiscpop.

International Association of Law Enforcement Intelligence Analysts (IALEIA)
www.ialeia.org/ [Accessed 27 April 2017].

Problem Oriented Policing
www.popcenter.org/about/?p=whatiscpop [Accessed 27 April 2017].

United Nations Office on Drugs and Crime – Organized Crime:
www.unodc.org/unodc/en/organized-crime/index.html?ref=menuside
[Accessed 27 April 2017].

TNTD/SPMU Publication Series

Vol. 1 Guidebook on Democratic Policing by the Senior Police Adviser to the OSCE Secretary General, SPMU Publication Series Vol. 1, 2nd Edition, Vienna, May 2008.

Vol. 2 Reference Guide to Criminal Procedure, SPMU Publication Series Vol. 2, Vienna, December 2006.

Vol. 3 Enhancing cooperation among police, prosecutors and judges in the fight against transnational organized crime. Project Report, SPMU Publication Series Vol. 3, Vienna, December 2007.

Vol. 4 Good Practice in Building Police-Public Partnerships by the Senior Police Adviser to the OSCE Secretary General, SPMU Publication Series Vol. 4, Vienna, May 2008.

Vol. 5 Good Practices in Basic Police Training – Curricula Aspects by the Senior Police Adviser to the OSCE Secretary General, SPMU Publication Series Vol. 5, Vienna, October 2008.

Vol. 6 Прекурсоры наркотических средств [Precursors Handbook], SPMU Publication Series Vol. 6, Vienna, November 2008.

Vol. 7 Implementation of Police-Related Programmes. Lessons Learned in South-Eastern Europe, SPMU Publication Series Vol. 7, Vienna, December 2008.

Vol. 8 Controlled Delivery Guidebook for South-East European Countries, SPMU Publication Series Vol. 8, Vienna, January 2009.

Vol. 9 Police and Roma and Sinti: Good Practices in Building Trust and Understanding, SPMU Publication Series Vol. 9, Vienna, April 2010.

Vol. 10 Trafficking in Human Beings: Identification of Potential and Presumed Victims. A Community Policing Approach, SPMU Publication Series Vol. 10, Vienna, June 2011.

Vol. 11 Police Reform within the Framework of Criminal Justice System Reform, TNTD/SPMU Publication Series Vol. 11, Vienna, July 2013.

Vol. 12 OSCE Resource Police Training Guide: Trafficking in Human Beings, TNTD/SPMU Publication Series Vol. 12, Vienna, July 2013.

Vol. 13 OSCE Guidebook on Intelligence-Led policing, TNTD/SPMU Publication Series Vol. 13, Vienna, July 2017.

Other police-related TNTD publications:

Human Rights In Counter-Terrorism Investigations. A Practical Manual For Law Enforcement Officers. Joint publication of the OSCE Office for Democratic Institutions and Human Rights (ODIHR) and TNTD, Warsaw, 2013.

Preventing Terrorism and Countering Violent Extremism and Radicalization that Lead to Terrorism. A Community-Policing Approach. Joint publication of ODIHR and TNTD, Vienna, February 2014.

Publications can be ordered directly from the TNTD/SPMU (spmu@osce.org) or downloaded from the POLIS website at: polis.osce.org/library

Follow OSCE

Organization for Security and Co-operation in Europe

OSCE Organization for Security and Co-operation in Europe