Ministry of Justice and Security

Subversion Threat Assessment Netherlands

2026

Strategic Knowledge Centre Subversive Crime

Colophon

The mission of the Strategic Knowledge Centre Subversive Crime is to bring together and interpret information and knowledge for a problem-oriented approach to subversive crime, with the aim of preventing societal disruption caused by organised crime. By providing insight into the threat posed by subversive organised crime, the SKC contributes to system-wide strategy development and (policy) follow-up for the integrated approach to subversive crime.

The **Subversion Threat Assessment Netherlands (STAN)** 2026 is the first publication in this series. In addition to the STAN, the SKC conducts other studies in the form of international and thematic research on subversive crime.

Numerous public and private organisations contributed to the development of the STAN.

All quotes originally in Dutch were translated by the author.

Version number 1, printed in 2026

View the digital version and our other publications here: www.skc-oc.nl

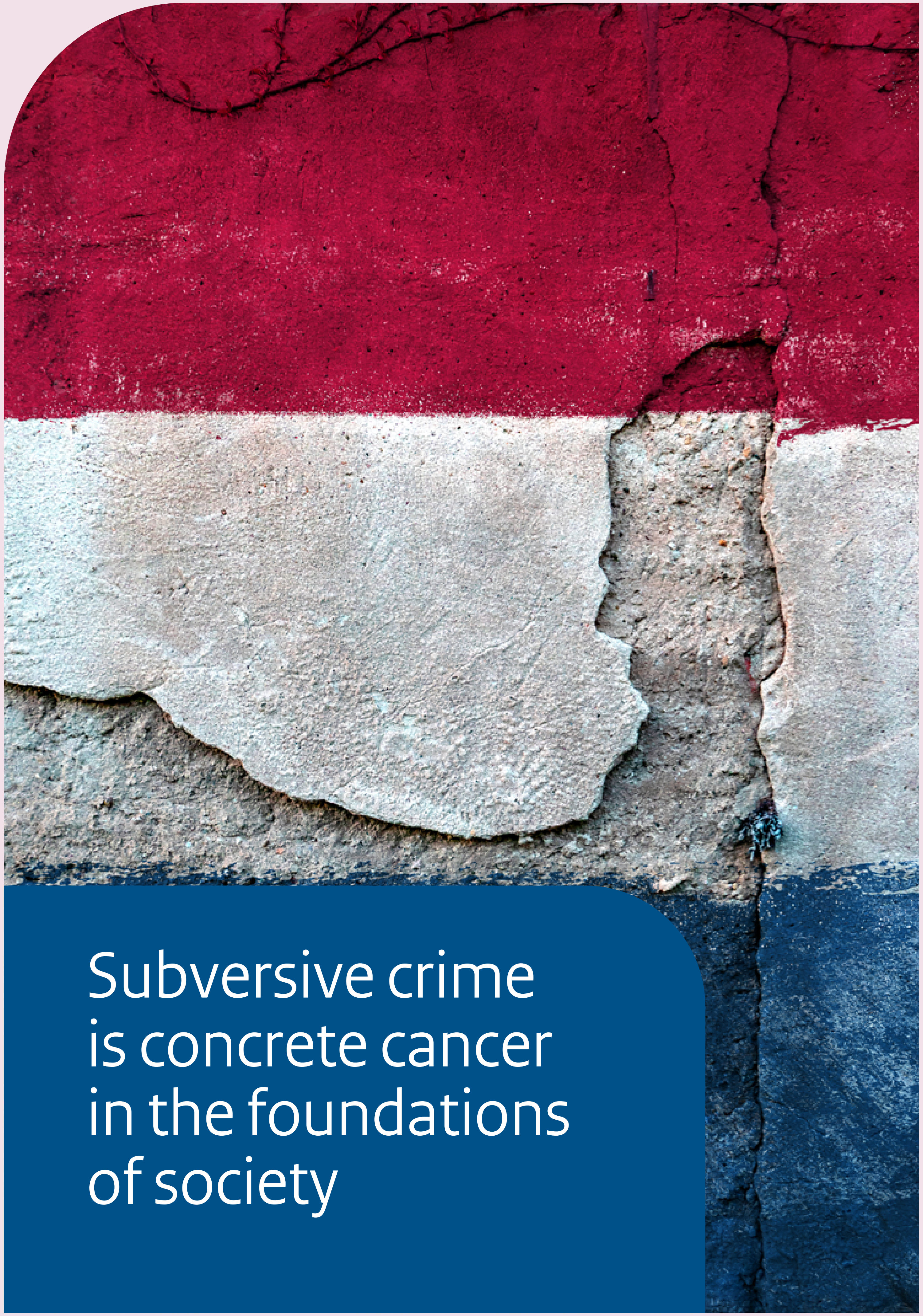
“Gutta cavat lapidem, non vi sed saepe cadendo”

- Ovid

The drop hollows out the stone, not by force, but by falling often.

Just as water slowly wears away stone, subversive crime often imperceptibly erodes the foundations of our society. That process is not always immediately visible, but its consequences are certainly real.

Table of Contents



Subversive crime is concrete cancer in the foundations of society

Executive summary

Subversive crime is concrete cancer in the foundations of society

Subversive crime by organised crime erodes the democratic rule of law in an insidious and often invisible manner and poses a threat to national security. The role of organised crime is increasing because criminal networks meet societal needs, through the involvement of citizens and companies in illegal activities, and through the manipulation of decision-making and the functioning of institutions. Furthermore, illegal proceeds find their way into the regular economy. At the same time, society may lose its grip on this dynamic due to its own vulnerabilities. The high degree of agility characteristic of organised crime makes an effective approach more complex.

Presented here is the first Subversion Threat Assessment Netherlands (STAN), which focuses specifically on subversive crime by organised crime. It provides an overarching and societal overview of the threat posed by this form of subversive crime to the Netherlands. The STAN is a substantive basis for strategy and policy development for the integrated approach to subversive crime.

In the context of subversive crime, a distinction can be made between subversive activities and subversive effects. The focus in the STAN is on subversive effects for the Netherlands, also referred to as harm. These are the result of subversive activities: the use of infrastructures by criminal networks. Examples include money laundering in economic infrastructures or the corruption of officials in political-administrative infrastructures. No explicit attention is paid to primary activities through which criminal networks illegally obtain money, such as drugs trafficking or people smuggling. The aim is to interpret subversive crime within the broad context of society rather than describing individual forms of criminality.

Five threats putting pressure on the Netherlands

The greatest danger is that the role of organised crime in society is increasing, while society is losing its grip due to its own vulnerabilities. This creates a “state within a state” through a self-reinforcing process: criminal networks expand their influence and power in economic sectors and neighbourhoods, they become increasingly elusive to supervision, investigation, and prosecution, they amass great fortunes, and more and more citizens and organisations become involved in criminal activities. Decision-making and institutional functioning are increasingly influenced, directly or indirectly, by criminal networks. Examples from several South American countries show that such developments can indeed occur.

Based on sources provided to the SKC or collected by the SKC itself, five threats have been identified that will shape the threat landscape for the coming years. These threats show what may lie ahead. Sometimes examples are already visible, but often they are an interpretation of weak signals or based on plausible reasoning. Those who focus exclusively on what is already happening are not sufficiently responding to future risks.

The threats stand on their own but can influence or reinforce each other. Other threats from the security domain also play a role, such as the digital threat and the threat posed by state actors.

This interconnectedness makes the threat landscape complex, dynamic, and diverse. Conversely, this interconnectedness also offers opportunities for an approach that does not focus on a single threat, but on several simultaneously and in conjunction with other security domains. In this way, resilience against subversive crime can be strengthened, while also contributing to resilience across the board.

Hereafter is an explanation of the threats. The full analysis can be found in chapter 7.

Schematic representation of the five threats for the Netherlands

Threat: Social safety net by organised crime

Criminal networks offer alternatives to ‘social services’ that are insufficiently accessible or available to citizens and companies. Examples include housing or physical protection, healthcare, loans, or medicines that can only be obtained by prescription. When criminal networks meet these needs, they not only obtain money illegally, but also increase their influence and power.

Structural and situational factors contribute to that need. Examples include a lack of housing in combination with financial hardship, or enterprises that face difficulties due to flooding. Some political choices and government policies also contribute to those needs; for instance, farmers who experience financial pressure due to regulations regarding nitrogen or manure, or measures for the fisheries sector.

Threat: Oil-spill effect of involvement in organised crime within society

Involvement in organised crime can spread like an oil spill throughout our society. There are numerous examples of participation in organised crime by, for example, young people, including in secondary schools and, in an isolated case, even in primary schools. Involvement varies in degree, and the initiative originates from both criminal networks, as well as from citizens or employees of organisations.

Various vulnerabilities and developments can – either individually or in combination – contribute to involvement. Examples include the financial appeal of organised crime combined with the desire for status and making quick money, the opportunities provided by digital platforms for establishing contacts, and financial, psychological and/or mental vulnerabilities. Limitations in the approach and in laws and regulations can contribute to an oil-spill effect, for instance because involvement is not detected in time or the drawing power of digital platforms is not countered.

Threat: Influencing decision-making and the functioning of institutions through structural manipulation by criminal networks

When criminal networks have built up significant interests and these face pressure, they will seek to manipulate decision-making and the functioning of institutions within society in a strategic and structural manner. If they succeed in this, criminal interests are taken into account -consciously or unconsciously- in decision-making and the functioning of institutions, for example, to avoid violence or other problems.

Manipulation is interpreted broadly in this context and takes various forms and degrees. It may consist of attempts to deliberately influence laws and regulations, administrative decision-making, law enforcement, and the performance of government tasks. Manipulation also includes engaging in a conflict with ‘adversaries’ by putting them under pressure, threatening them, or by spreading disinformation about them. Adversaries may be criminal rivals. Officials of the rule of law are also considered adversaries, such as police officers, judges, public prosecutors, supervisors, administrators, politicians, journalists, lawyers, and/or others from society, including gatekeepers and companies or citizens.

Characteristic of organised crime is the threat of or use of violence. There are concerning examples of the use of violence in the Netherlands: the assassination attempt on the brother of a crown witness, his lawyer, and crime journalist Peter R. de Vries, who was also an advisor to that crown witness. In 2022, the media even reported possible criminal plans for an attack or kidnapping of the crown princess and the then-prime minister Rutte, as well as a foiled kidnapping of the Belgian Minister of Justice.

Various system vulnerabilities make the detection of (indications of) manipulation complex. These are related to limitations in the approach of combatting crime and in laws and regulations, particularly concerning the exchange and processing of information about such indications. This also involves low awareness of, for example

– but not exclusively – vulnerabilities to corruption and the lack of or minimal reporting of corrupt contacts or recruitment practices. Technological developments offer opportunities, more specifically through, for example, the use of drones in the application of violence, the development of digital platforms for assigning tasks, and Artificial Intelligence (AI) for generating advanced disinformation.

Threat: Illegal proceeds find their way into society through the diverse use of financial channels

Criminal networks have diverse and many opportunities to use financial channels, causing illegal proceeds to be mixed with legal proceeds and find their way into society. On the one hand, they must make payments and secure their obtained income. On the other hand, they must legitimize money flows in order to spend the money and avoid monitoring and investigation. In doing so, they make use of traditional banking infrastructures, new often global and digital financial infrastructures such as crypto platforms, and underground banking. This diversification enables criminal networks to set up increasingly sophisticated money laundering schemes.

Criminal networks already make extensive use of diverse financial channels. They continue to adapt to new developments to achieve their goals and mitigate risks. For legislation and regulation and the enforcement thereof, it is not only a challenge to keep pace with developments, but also to take into account the often global nature of those channels, the complexity of money laundering methods, and limitations in data sharing. The ease with which criminals can establish complex structures of (inter)national legal entities constitutes an additional vulnerability.

Threat: Cumulative harm due to the intertwining of criminal networks with ideological or state actors

Activities by criminal networks, state actors (such as sabotage by foreign intelligence services), and ideologically motivated actors (including terrorist attacks), each leads to harm in their own right. Additional harm arises when criminal networks collaborate with ideologically motivated or state actors or provide each other with assistance. In the current geopolitical context, it is attractive for state actors to deploy criminal networks as an 'instrument' in so-called hybrid warfare. Conversely, criminal networks can benefit when they (unwittingly) provide services or products to state actors. (Unwitting) collaboration between criminal and ideologically motivated actors also offers potential mutual benefits. For criminal networks operating in Europe and the Netherlands it is more plausible that there is an unintended facilitation via fluid networks than there is a conscious and/or active collaboration.

There are examples of cooperation between state and criminal actors. Well-known is the cooperation between Russian state actors and Russian cybercriminals. Also well-known are the assassinations of opponents of the Iranian regime in Western countries by criminals acting on behalf of Iran. And there are also examples of the provision of services between ideological actors and organised crime.

Subversive crime is a threat to national security

Subversive crime by organised crime is a threat to national security. When the threats manifest, they impact - each individually and especially in combination - one or more national security interests. In the STAN, five types of subversive effects have been chosen, also referred to as harm: economic, political-administrative, social and ecological harm, and harm to the international reputation of the Netherlands. For the relationship between threats and national security interests, see figure 0.1.

When threats materialize, they primarily compromise the national security interests of economic security and social and political stability. The extent to and the manner in which harm occurs is heavily dependent on how the threat actually manifests. After all, it matters significantly whether, for example, the government has lost control in a single neighbourhood in one city or in dozens of neighbourhoods across several cities. It also matters whether, for instance, there is large-scale use of violence, extensive involvement of citizens and businesses in those neighbourhoods, or not.

Subversive effects also influence vulnerabilities that criminal networks exploit. This results in a self-reinforcing mechanism: effects are not only the consequence of subversive activities but also contribute to them. Corruption, for example, erodes trust in the government. As a result, the willingness to report corruption may decrease. Consequently, the government misses important signals of corruption, and the harm thus insidiously increases. In practice, this concerns a dynamic – rather than 'linear' – interaction between various subversive activities, effects, and system vulnerabilities.

Relationship between national security interests, subversive effects and threats

- National security interests
- Threat
  - **Social safety net** by organised crime
  - Oil-spill effect of **involvement** in organised crime within society
  - Influencing decision-making and the functioning of institutions through structural **manipulation** by criminal networks
  - **Illegal proceeds** find their way into society through diverse use of financial channels
  - Cumulative harm due to the **intertwining** of criminal networks with ideological or state actors
- Type of harm

Figure 0.1

Criminal networks use infrastructures to achieve their goals

Criminal networks potentially use all Dutch infrastructures that are also attractive to legal companies. In the STAN, a distinction is made between: economic, political-administrative, social, ecological and international infrastructures. Criminal networks use these both individually and in combination to achieve their goals. The Netherlands has many attractive infrastructures and sectors. Locations where concentrations of infrastructures occur are particularly attractive to criminal networks. The Netherlands has numerous of such concentrations, such as the mainports: Schiphol Airport, the ports of Rotterdam, the North Sea Canal area, the area Zeeland and West Brabant, and flower auctions/the ornamental horticulture sector. Furthermore, concentrations exist in and at smaller seaports and airports, and in the financial and legal sector of the Amsterdam's business district (Zuidas).

Criminal networks primarily use Dutch infrastructures for illegal gain. Derived from this, various (sub) objectives can be distinguished for which they use these infrastructures:

1. Supporting/continuing business operations.
2. Protecting and shielding operations and finances.
3. Maintaining or expanding power and reputation.
4. Maintaining or expanding network(s).
5. Acquiring and manipulating information.
6. Obtaining access to locations, resources and official documents.

The goals of criminal networks can be achieved through a wide range of activities. To obtain information, for example, they may make use of corrupt officials, but they could also obtain information through cyberattacks. Conversely, a single type of activity may contribute to the achievement of one or more goals. Through corrupt officials, they can also obtain official documents or attempt to influence decision-making. Therefore, measures taken by the government and companies to curb one type of activity can be partially offset by criminal networks by choosing other activities to achieve the same result.

Making a distinction between the upper and underworld suggests that there are two separate worlds, but the reality is blurred. After all, criminal networks use infrastructures within society. This results in complex and dynamic connections between organised crime and society. This form of crime does not only involve vulnerable individuals, but also people you would not typically expect. The initiative certainly does not come solely from criminal networks but can also originate from society. Moreover, the demand for illegal products or services often comes from society and not only from criminals.

System vulnerabilities offer opportunities for organised crime

Whether criminal networks actually use infrastructures depends not only on their attractiveness, but also on characteristics that make infrastructures vulnerable: system vulnerabilities. Individually, but especially in combination, these provide opportunities for organised crime (see box 0.1 and section 3.3).

Developments offer opportunities for organised crime

Some broader developments in society, both individually and in combination, create new opportunities for organised crime (see box 0.2 and chapter 5). These potentially create new possibilities in illicit markets or for subversive activities. They also influence system vulnerabilities. As a result, criminal networks may benefit for shorter or longer periods of time.

Tension between the agility of criminal networks and limitations in the approach

There is a tension between the agility of criminal networks on the one hand and limitations in the approach of combatting criminal networks on the other. This tension makes controlling subversive crime complex. Criminal networks respond strategically or opportunistically to developments, opportunities, and the attractiveness of infrastructures, system vulnerabilities, and risks. They have many options to achieve their goals. As a result, they are able to easily and quickly replace activities and use other infrastructures to achieve the same goal. Conversely, it takes time before society detects changes in criminal behaviour and can or may respond to them. Furthermore, there is a waterbed effect: pressure on one phenomenon leads to displacement to another.

System vulnerabilities that have emerged (non-exhaustive)

System vulnerabilities	Description or examples
Unintentional government facilitation	• The emergence of a waterbed effect because policy or an approach leads to shifts toward other phenomena, locations, or policy domains. • A balancing of interests within policy on organised crime or crime in a broad sense, but also between policy domains such as security, economy, housing, or health. • Policy development without taking criminogenic effects into account, such as the privatisation or liberalisation of certain markets without monitoring potential crime risks, including the possibility of substantial misuse of government funds.
Limitations in the approach to subversive crime	• Limitations in cooperation, including a lack of coherence in the approach. • Limitations in data sharing and processing. • Reactive nature of government action. • Limitations in the international aspects of the approach.
Restrictions in laws and regulations	• Complexity of and gaps in laws and regulations. • Complexity of privacy legislation.
Normalisation of crime	• Social acceptance of drug use and dealing within some groups in Dutch society. • Turning a blind eye to crime or participating in it.
Reduced trust of citizens in government and in each other	• Communities with little trust in the government, but with a great deal of trust in fellow citizens, can develop into safe havens where the government is seen as an opponent rather than an ally.
Vulnerabilities in business processes	• Vulnerabilities in 'employee processes', for example in screening. • Vulnerabilities in ICT and information processes, for example basic cybersecurity measures not taken. • Vulnerabilities in the issuance process of documents that are crucial for criminal networks, for example access passes or identity documents.
Complexity controlling the misuse of dual-use sectors and means	• Large-scale and targeted global trade in sensitive personal data. • Dual-use equipment, including technical equipment suitable for intelligence gathering.
Vulnerabilities within groups, neighbourhoods and sectors	• Financial, psychological and/or mental vulnerabilities. Examples include: financial vulnerabilities due to shrinkage in sectors such as fisheries, addiction issues, family problems or problems at school. • A closed/isolated culture. Examples include a culture of silence or fear, an inner circle culture and a taboo on reporting, for example, corruption out of fear of reputational damage.

Box 0.1

Developments that offer opportunities for organised crime (non-exhaustive)

Developments	Relevance
The deployment of unmanned systems, including drones	These systems are suitable for various activities: for smuggling, as a means of espionage, and for surveillance or the commission of violence. Intercepting these systems is complex and developments are moving quickly, especially in the war against Ukraine.
Developments of digital platforms for all kinds of activities	Digital platforms are attractive for business operations, shielding, the manipulation and recruitment of individuals, and obtaining information. Via digital platforms, criminal networks can come into contact with many people remotely and on a large scale, while remaining relatively anonymous and with few risks. Gaining control over these activities of criminal networks on digital platforms is complex.
Artificial Intelligence (AI)	Criminal networks can utilize AI in various ways: for various forms of fraud, the creation of deepfakes and phishing messages, analysing large datasets to identify potential targets, spreading disinformation, and supporting the development of new (synthetic) drugs.
Geopolitical developments	State actors may deploy criminal networks for hybrid warfare. In the context of geopolitical tensions, international sanctions are applied to countries, and countries impose import tariffs on each other. Trade restrictions offer opportunities for smuggling. Geopolitical tensions create pressure on international cooperation, from which organised crime can profit. A termination of the war against Ukraine also offers opportunities for criminal networks.
Developments in digital payments	New payment methods and channels are emerging that offer opportunities for diversification.
Desire to get rich quickly and prioritizing personal gratification	Especially via digital platforms, users showcase a luxurious lifestyle or commodities, and influencers proclaim that you can earn a lot of money quickly with minimal effort. In this context, organised crime exerts an appeal.
Ecological developments	Climate change, scarcity of raw materials, biodiversity loss and the energy transition not only offer opportunities for illicit markets, but can also increase dependencies and/or vulnerabilities from which criminal networks can profit.

Box 0.2

Concluding remarks

Subversive crime is a so-called *wicked problem*, a problem characterized by complexity, uncertainty, and conflicting values. After all, the landscape of subversive crime is complex, dynamic, and diverse, and it affects everyone. Many factors exert an influence: the goals of criminal networks, the opportunities and attractiveness of infrastructures, system vulnerabilities, societal developments, and all of these in varying combinations. These also vary depending on the geographic area and circumstances. Furthermore, subversive crime reinforces societal problems, and vice versa. Criminal networks respond to all of this opportunistically and strategically.

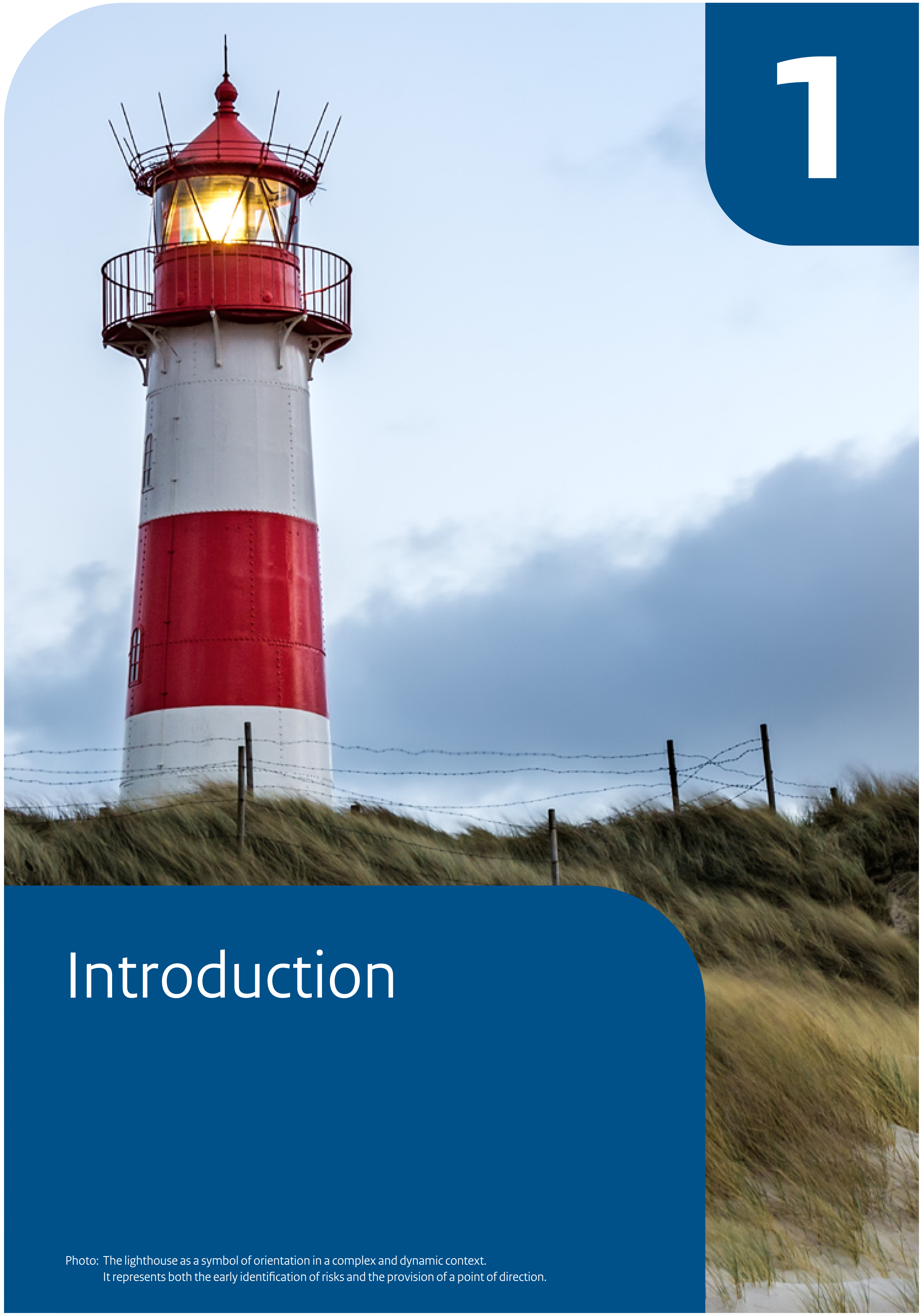
Complex problems rarely offer *quick wins*. A characteristic feature is also that these problems do not align seamlessly with the responsibilities and powers of specific government or public organisations. This makes a decisive approach to combat subversive crime difficult. Nevertheless, efforts to increase the resilience of Dutch society also contributes to resilience against subversive crime, and vice versa. This applies, for example, to measures in ports against the use of drones by state actors: these measures also help against the use of drones by criminals.

One factor cannot be emphasized enough in this context: the astronomical sums of money circulating in organised crime. For good reason, there is a proverb: “money opens many doors”. During court cases, it becomes clear which enormous amounts are earned or laundered. Mapping these is complex. And, despite numerous efforts, seizing criminal money remains extremely difficult.

The period during which criminal networks can operate contributes to the threat they pose. According to Europol, 34% of criminal networks have been active for more than 10 years and are able to maintain their influence and power. Because the Netherlands Police had access to encrypted communications between criminals for a period of time, criminal networks came on the radar that otherwise could have continued their activities for years. But what if the source of the encrypted communications has dried up? Once arrested, prosecution and adjudication take many more years, and afterwards, some criminals continue their criminal activity from detention.

Looking back at the analysis, several topics have emerged that are important for a comprehensive overview, but about which relatively little is known. This is certainly true for the extent to which organised crime exerts influence on and holds a position of power in Dutch society. That this occurs in certain neighbourhoods and sectors is highly plausible. Some fragmented examples have been presented in this regard, but a complete overview is unavailable. Attention has also been paid to the influence of digital platforms. Although research has been conducted from other perspectives, additional research could provide a better overview. This is equally true for the extent to which and how unmanned systems, such as drones, affect the threat landscape of subversive crime.

In this STAN, as comprehensive a picture as possible has been sketched of subversive crime by organised crime. It offers leverage points to view the phenomenon more holistically and from the perspective of society, rather than solely from the perspective of organised crime. In this way, the STAN can contribute not only to the development of preventive measures, but also to early detection of or combating organised crime, in order to limit the harm to society.



1

Introduction

Photo: The lighthouse as a symbol of orientation in a complex and dynamic context. It represents both the early identification of risks and the provision of a point of direction.

1.1 Context

The Directorate-General for Subversive Crime (DGO) of the Ministry of Justice and Security, acting as the coordinating commissioning party, has commissioned the Strategic Knowledge Centre Subversive Crime (SKC) to produce a "Subversion Threat Assessment Netherlands" (STAN) focusing on organised crime. Unlike security issues such as terrorism and extremism, cybersecurity and state threats, no national threat assessment yet exists regarding subversive crime by organised crime.

1.2 Purpose and target group

The purpose of the STAN is to provide insight at a national level into:

The threat to the Netherlands of subversive crime by organised crime for the purpose of system-wide strategic development and subsequent policy implementation within an integrated approach.

The STAN primarily focuses on politicians, civil servants, and administrators who are responsible for strategy formation and (policy) follow-up (hereinafter: strategic follow-up). This group bears explicit responsibility for achieving that follow-up and for mobilizing crucial public and private parties in the approach to subversive crime.

The approach to subversive crime affects the tasks of many organisations. The target group therefore also consists of executives and employees who play a role in translating this into the objectives for those organisations. This includes, among others, national, regional, and local public system partners, such as the Netherlands Police, Royal Netherlands Marechaussee (KMar), Customs Administration of the Netherlands, Dutch Tax Administration, the Fiscal Intelligence and Investigation Service (FIOD) and other Specialized investigation services (BODs), Netherlands Public Prosecution Service (OM), supervisors, provinces, and municipalities. These system partners collaborate, whether or not within Regional Information and Expertise Centres (RIECs) and the National Information and Expertise Centre (LIEC) or in other partnerships, such as around the various mainports and in the National Crime Prevention Platform, the Care & Safety Houses, and the Financial Expertise Centre (FEC). Healthcare and educational institutions and organisations in civil society, such as industry and professional associations, are also part of the target group. Finally, the STAN informs private parties, academics, journalists, citizens, and other interested parties.

1.3 Principles of the STAN

The following principles apply to the STAN:

1. The STAN provides an integrated, multidisciplinary overview of society- and government-wide subversive effects. It is therefore not about a criminal law perspective.

2. The STAN provides a national overview and does not focus on specific sectors or regions. However, examples from specific sectors or regions have been included in the analysis. The STAN does not focus on the Caribbean Netherlands and the Caribbean part of the Kingdom.

3. The STAN is a so-called qualitative analysis. In a qualitative analysis, phenomena are analysed in depth in their complexity and interconnectedness.[1] Findings in the STAN are substantiated based on arguments, reasoned from sources provided by partners, public sources and consulted experts, and/or by analogy.

4. No use was made of operational information or specific case studies from, for example, ongoing criminal investigations during the preparation of this document.

5. The STAN contains no policy recommendations and/or a policy evaluation.

6. The STAN was independently developed within the framework of the commissioned assignment.

1.4 Scope and key terms

In the STAN, the choice was made for "Subversive crime by organised crime" instead of "organised, subversive crime" or other variants with the words organised, crime, and subversive crime. The point of departure is that organised crime, by definition, constitutes subversive crime.[2] In the still authoritative definition of organised crime by the Fijnaut research group (see box 1.1), "serious consequences for society" is an important component. Subversive crime—including subversive crime by organised crime—is a broader and overarching concept. The concept of subversive crime is even more comprehensive and is not limited to crime.[3] Examples of this are subversive crime by state actors or terrorists.

Subversive crime by organised crime has been operationalised by the SKC into separate components (see figure 1.1). In the case of subversive crime, a first distinction can be made between subversive activities and subversive effects resulting from those activities.[4] Subversive activities can be divided into a) primary activities through which criminal networks illegally obtain money and b) the use of infrastructures by criminal networks in support of those primary activities. Infrastructure refers to economic, political-administrative, social, ecological, and international infrastructures, both offline and online. When reference is made to subversive activities in the STAN, this is limited to b: "the use of infrastructures by criminal networks". Examples include money laundering in economic infrastructures or the application of violence against administrators in political-administrative infrastructures. The focus in the STAN is therefore not on, for example, drugs trafficking, cigarette smuggling or arms trafficking. This is in contrast to many other reports on subversion, which focus on those illegal activities. Subversive activities are carried out by criminal networks. Whether criminal networks use infrastructures depends not only on the opportunities and attractiveness for achieving their goals, but also on

Focus threat assessment

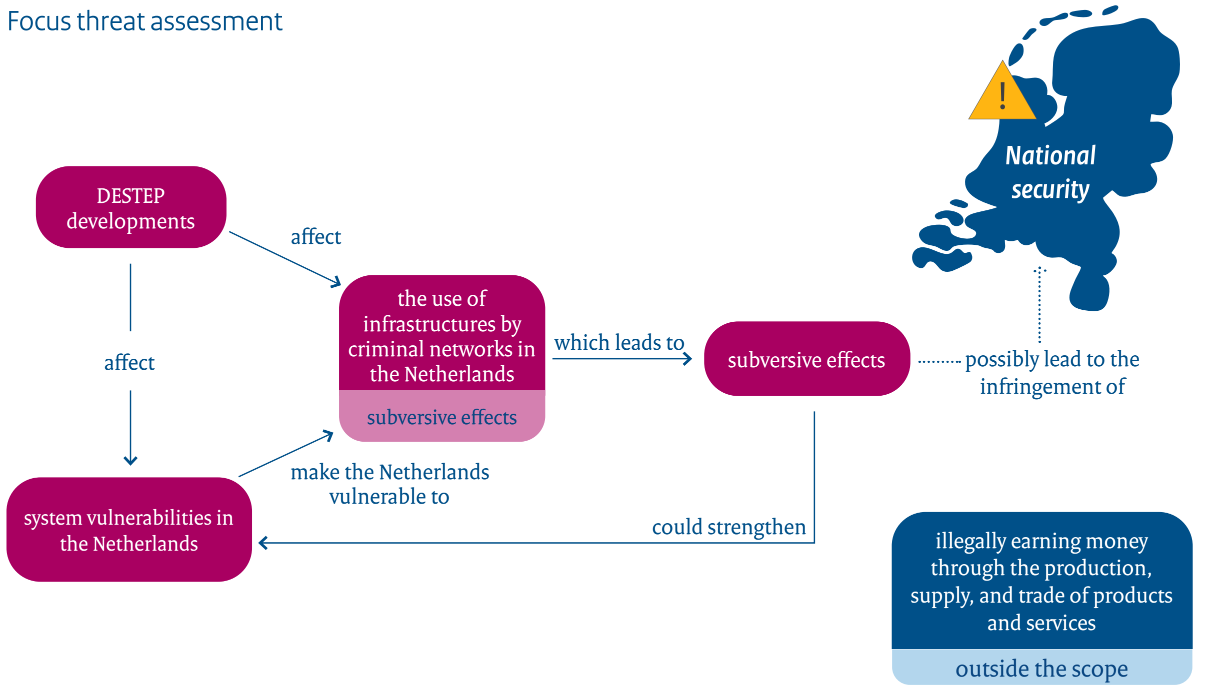


Figure 1.1

characteristics that make them vulnerable to this, further referred to as 'system vulnerabilities'. Demographic, economic, social, technological, ecological, and political developments (DESTEP developments) influence subversive activities and system vulnerabilities. Insight into these makes the analysis more forward-looking.

While many documents on subversive crime by organised crime focus primarily on subversive activity, for the STAN, the focus has been placed primarily on the subversive effects, also referred to as harm. This provides a better insight into this harm for strategic follow-up. On this basis, interests can, be weighed.

The focus is on a "clustered subversive effect" (see box 1.1). This aligns with the focus on subversive effects. Clustering was chosen due to the so-called many-to-many relationships that exist between activities and effects (see paragraph 6.1). Furthermore, the objective and the target group impose requirements on the level of abstraction of threats.

The concept of threat has been operationalized for the target group and the purpose of the STAN. In principle, each of the aforementioned components can serve as the starting point for the identification of threats:

- **Development**: acceptance of cryptocurrencies as a means of payment for the purchase of expensive commodities.
- **System vulnerability:** absence of a legal basis for the reporting obligation for cryptocurrency payments.
- **Activity:** money laundering through the purchase of expensive cars with payments in cryptocurrencies.
- **Effect:** impairment of the vitality of economic infrastructures.
- **National security interests:** undermining of economic security.

The definitions are detailed below, including the focus and scope.

Key definitions

Criminal network:
"Network in which individuals collaborate with acquaintances and introduce one another to others to carry out criminal activities; due to the existence of social relations, bridges can also be built between criminal networks in different countries".[5]
For a detailed explanation, see paragraph 2.1.

DESTEP developments:
demographic, economic, social, technological, ecological and political developments that may influence system vulnerabilities and subversive activities. Examples include technological developments in digital payment traffic.

Threat (for the Netherlands):
a clustered subversive effect on Dutch society resulting from the use of Dutch infrastructures by Criminal networks.

Organised crime:
"Organised crime occurs when groups primarily focused on illegal gain systematically commit crimes with serious consequences for society, and are able to shield these crimes in a relatively effective manner, particularly by demonstrating a willingness to use physical violence or to neutralize persons through corruption."[6]

Infrastructure:
a set of facilities through which a country can function properly. The following are distinguished: economic, political-administrative, social, ecological and international infrastructures.

National security:
"By national security, we mean the protection of our national security interests against threats that can harm these interests and thereby cause societal disruption."[7]

National security interests:
territorial security, physical security, economic security, ecological security, social and political stability and international legal order. See paragraph 7.1.

The subversive effect of organised crime is a (either short- or long-term) impairment of the legal and intended functioning of political-administrative, economic, social and ecological infrastructures as a result of subversive activities and "harm to the international reputation of the Netherlands".
Scope:
- This concerns effects in the Netherlands: after all, it requires specific knowledge of other countries to be able to assess those effects there.
- Ultimately resulting in the potential impairment of national security interests. Potential impairment of national security is not a priori considered the lower limit for the identification of subversive effects.

Subversive activity by organised crime concerns the use of infrastructures by criminal networks. This type of activity is often carried out in support of primary activities (such as people smuggling) or otherwise stems from these. Examples include activities such as the corruption of government officials (political administrative infrastructure) or money laundering (economic infrastructure). Scope: activities in the Netherlands or abroad with subversive effects in the Netherlands.

Subversive crime concerns the harmful effects for society resulting from the activities of actors. Scope: in the STAN, this refers to subversive crime by organised crime. In this context, a distinction is made between subversive activities and effects.

Legal entity: organisation, entity, company, natural person acting as a company, or institution that has rights and obligations and can be used for criminal activities.

System vulnerabilities:
influenceable factors or characteristics that make infrastructures vulnerable to use by criminal networks. An example is "financial instability in the agricultural sector", which can lower the resistance of farmers to accept an offer from criminals to make space available. Non-influenceable factors or characteristics, such as the global role of the port of Rotterdam, are not considered system vulnerabilities.

Box 1.1

1.5 Main question and research questions

The main question underlying the STAN is:

What threat does subversion by organised crime pose to the Netherlands?

The research questions derived from the main question are:

1. In what way do criminal networks use Dutch infrastructures?
2. Which types of Dutch infrastructures do criminal networks use?
3. Which types of system vulnerabilities make Dutch infrastructures susceptible to use by criminal networks?
4. Which DESTEP developments primarily influence system vulnerabilities and subversive activities?
5. Which subversive effects can result from (combinations of) subversive activities?
6. From which combination of subversive effects does a threat emanate?

1.6 Reading guide

The STAN consists of the previous chapter, in which the main findings are articulated, and of in-depth chapters. The previous chapter provides the unifying thread running through the remaining chapters. To get a clear picture, reading the other chapters is strongly recommended. The core of a chapter is briefly presented at the beginning of each chapter. The reader with limited time is advised to read chapter 7, in which the threats are elaborated.

In the in-depth chapters, answers are provided to the research questions:

- **Chapter 2** Organised crime is not separate from society. This chapter describes assumptions about organised crime.
- **Chapter 3** Criminal networks use attractive and vulnerable infrastructures. In this chapter, subversive activities, infrastructures and system vulnerabilities are elaborated. This chapter provides answers to research questions 1 through 3.
- **Chapter 4** The involvement of youth and criminal interference: interplay between factors. This chapter addresses common subversive activities: the recruitment and use of youth, corruption, infiltration, and the use of violence. This shows that although components of subversive crime can be analytically separated, in practice, it is often a complex and dynamic interplay between them.
- **Chapter 5** New opportunities for organised crime. In this chapter, several DESTEP developments are described that influence subversive activities and system vulnerabilities. This chapter provides the answer to research question 4.
- **Chapter 6** Dynamic interaction between subversive effects and activities. This chapter answers research question 5.
- **Chapter 7** Threats. This chapter answers research question 6.
- **Appendix 1** contains an account of the development of the STAN.
- **Appendix 2** contains sources and references.

2

Organised crime is not separate from society

Photo: A container ship in the Port of Rotterdam. Criminal networks strategically recruit contacts, such as a port employee whose position enables the passage of a container.

Organised crime is not separate from society. Criminal networks operate as 'criminal enterprises' in illicit markets where supply and demand meet. They meet a demand from citizens and companies that legal organisations and the government do not meet, do not meet to a sufficient extent, or only meet at higher prices or under strict conditions. Criminal networks are agile and respond to developments, opportunities, and risks within and between various countries. They appear in various forms and are dynamic and fluid in nature.

2.1 Organised crime committed by criminal networks

2.1.1 Criminal networks: diverse and dynamic collaborations

Criminal networks are dynamic and diverse in their organisational structure, size, nationality, and cultural composition.[8] They may consist of permanent members and external actors who are often not affiliated with a single criminal network on a long-term basis.[9] Some have a stable core (inner circle) of one or more key figures with a fluctuating outer circle. Others are decentralized and primarily consist of loose, temporary relationships.[10] Additionally, there are criminal networks that operate locally or regionally, but criminal networks often do not adhere to territorial borders.[11] This is directly related to the predominantly international nature of organised crime.[12] Furthermore, not all individuals need to know each other or work directly with one another.[13]

2.1.2 Criminal networks often expand their network structures through digital platforms, acquaintances, friends, family, and (former) fellow inmates

Just like legal enterprises, criminal networks consist of individuals, collaborate – whether or not on a long-term basis - with other individuals, and have customers, service providers, and suppliers. Both pre-existing and newly formed social ties facilitate the initiation and continuation of criminal enterprises. Acquaintance, friendship, and family ties are important because they create trust in a high risk, unregulated environment.[14] Involvement in a criminal network can begin through social ties and deepen: the longer someone is active, the more this person builds up their own contacts, assets, and knowledge, allowing them to attract new people themselves.[15]

New recruitment channels emerge in diverse social contexts, including (vulnerable) neighbourhoods, work, school, associations, and motorcycle clubs. These social settings also provide access to strategic contacts, such as a port worker who, through their position, can facilitate the passage of a container.[16] Prisons can also serve as social meeting places.[17] Inmates form new relationships during detention.[18] Especially in recent years, digital platforms also offer many opportunities to tap into new contacts (see further paragraph 5.1.1).

2.2 Criminal networks operate as enterprises in illicit markets

2.2.1 Criminal networks meet (inter) national demand for illegal products and/or services

Criminal networks can be regarded as criminal enterprises operating in (international) illicit markets. Just like legal enterprises, they meet a demand for a commodity or service. One difference is that criminal networks meet needs that legal organisations or the government do not meet at all, cannot meet for everyone, or produce or deliver at higher costs than criminal networks (see box 2.1). The product or service itself, or parts of the business process, are criminal or strictly regulated and are offered or executed in violation of applicable laws and regulations.[19]

Although drugs trafficking - both focused on import, transit and export and on distribution and production within the Netherlands - plays a prominent role, criminal networks are not limited to this. As shown in box 2.1, they may also be involved in various forms of fraud (such as fraud between private individuals (horizontal fraud) and fraud against the state (vertical fraud)), financial-economic crime, environmental crime, human trafficking, arms trafficking, or other illegal services.

Examples of products and services of criminal networks

Categories of products and services	Examples (non-exhaustive)
Prohibited products and services	Drugs and prohibited plant and animal species.
Strictly regulated products and services	Weapons, medicines, e-cigarettes and gambling services.
Unique and scarce products	Art objects, human organs.
Forgeries	Fake identity documents and means of payment.
Products and services that violate market regulation rules	Excise goods (such as cigarettes), illegal waste processing, commodities used for VAT carousel fraud.
Stolen commodities	Stolen cars, credit card details or identity data.
Manipulated or misleadingly offered commodities	Meat originating from cows with growth hormones or forms of investment with high (fictitious) returns.
Proceeds of crime	Proof of ownership of land on the moon or other symbolic exclusive objects, or luxury commodities (such as jewellery and designer items).
Provided a 'social safety net'	Renting out homes, employer of migrant workers, and providing loans (see paragraph 7.2).

Box 2.1

The nature of the activities can vary and dependents on market opportunities, expertise within the network, and collaborative relationships. Moreover, criminal networks can be active in multiple criminal domains simultaneously. For example, in the case of vertical fraud – fraud in which the government is the victim – criminals certainly do not focus solely on a specific scheme, such as an environmental or healthcare subsidy, a reimbursement option, a benefit, or a tax regulation. Their primary objective is to obtain money illegally as quickly and efficiently as possible.[20]

Specific types of offences are not explicitly explained in the STAN, but are sometimes used as a basis and explanation for activities, system vulnerabilities, and effects.

2.2.2 The primary goal of criminal networks is financial gain

Financial gain as a goal for criminal networks is inherent in the definition that serves as the basis for the STAN. This objective is also supported by a meta-analysis of studies examining the motives of individuals involved in organised crime.[21] The capacity of criminal networks to amass large sums of money is illustrated by, according to the Statistics Netherlands (CBS), €15.5 billion was generated within national borders in 2021 from the production of and trade in cocaine, synthetic drugs, and cannabis alone (see paragraph 6.6). Court cases also reveal the astronomical sums that some manage to amass or launder. However, not everyone is successful in illicit markets. While according to the Netherlands Police a small number of criminals managed to build up wealth, many others did not. They were left with earnings that can be categorized as subsistence income. A portion of the criminal proceeds was spent on 'business costs'. Moreover, the majority fail to build up sufficient criminal wealth to make long-term investments in society. This includes, for example, the purchase of real estate, whether for personal use or as an investment, the establishment of a legitimate business, or the maintenance of offshore bank accounts to accumulate wealth beyond the reach of government authorities.[22]

To achieve financial gain as a goal, various other (sub) goals can be analytically distinguished (see paragraph 3.1). However, non-material goals can also be identified as motives for engaging in organised crime. For example, involvement can give someone a sense of belonging.[23] Individuals join and belong to an alternative (illegal) subculture, within which individuals share the same goals and/or norms and values.[24] Involvement can therefore become a way of life. Additionally, needs such as status, excitement, and pleasure can be motives.[25] When individuals perceive that they cannot achieve their goals through legal means, organised crime can become an attractive alternative path to social and economic success.[26] Legal ways to achieve non-material needs such as status and material needs such as money are not accessible to everyone to the same extent.[27] The perception of, or actual unequal access to, education, the labour market, and resources, as well as regional differences and discrimination, limit social opportunities for some groups.[28]

2.2.3 Criminal networks must overcome obstacles of illegality

Criminal networks operate in a different reality than legal enterprises. Due to the illegal nature of their activities, they cannot be guided solely by market forces or economic motives[29] (see paragraph 3.1 below). They also operate in a high-risk environment characterized by significant financial interests without formal rules or safeguards, such as contracts[30] or insurance. Furthermore, conflicts cannot be settled through formal institutions such as courts.[31] Having and building social relationships is of essential importance to overcome these obstacles (see paragraph 2.1.2.). Although (creating) mutual trust is important, the threat or use of violence remains a tool in the 'toolbox' to enforce or reinforce agreements.[32]

2.2.4 Criminal networks are dependent and are part of (inter)national legal and illegal ecosystems

Criminal networks operate within an (inter)national ecosystem that encompasses both the legal and illegal worlds. Organised crime cannot function without the opportunities provided by legal infrastructures.[33] For example, criminal networks use legal infrastructures for their activities; ranging from transport modalities (such as trucks, containers, ships and drones) and utilities (such as electricity and internet and telecom connections) to legal entities. In addition, they involve officials who are attractive to them because of the opportunities afforded by their position or function[34] (see paragraph 7.3).

Activities are not always carried out by individual criminal networks themselves but are also outsourced to others.[35] Activities are not always carried out by individual criminal networks themselves, but are also outsourced to others.[36] In the case of drug crime in the Netherlands, for example, there is a strong interconnection between various criminal networks.[37] Examples of activities that are outsourced include the hiring of professional money launderers, as well as intermediaries who arrange persons for the storage of drugs or the perpetration of violence.[38] In addition, there are criminal networks that offer their services to other criminal networks; for some, this is their primary activity,[39] also referred to as crime-as-a-service. An example of this is the outsourcing of the corruption of officials to so-called corruption brokers. They possess their own network of already corrupted contacts and serve multiple criminal networks, without being a permanent part of one specific criminal network.[40] In doing so, they operate as independent service providers within a criminal market of supply and demand.

Violence for hire

In an interview at the end of 2025, the head of Serious and Organised Crime at Europol stated that investigation services in the Netherlands have identified more than a hundred recruiters who approach young people via social media to commit murders, kidnappings, and explosions. According to Europol, this also includes fixers who arrange weapons or getaway cars. Each of these recruiters has up to a hundred young people or young men under their thumb who can carry out acts of violence. Foreign gangs hire Dutch nationals for acts of violence to remain under the radar themselves. But it also happens the other way around. This violence on demand (violence-as-a-service) emerged in recent years in Sweden, which is struggling with extreme gang violence. Subsequently, the phenomenon spread like wildfire across the rest of Europe.[42]

Box 2.2

Partly due to the interconnection between criminal individuals or criminal networks, organised crime in the Netherlands, is according to the Dutch police, poly-criminal in nature: criminal enterprises are generally active in multiple criminal domains, such as trafficking in various narcotics and the commission of property crimes property crimes. Additionally, according to the Netherlands Police, there are no monopolistic positions. They are typically involved in multiple and different criminal projects. At the same time, criminal projects are outsourced in stages. There is significant competition, and a large network of criminal actors enables the criminal process to be broken down more easily into separate components and outsourced.[41]

2.3 Criminal networks respond to developments, opportunities and risks in the (il)legal world

Criminal networks capitalize on developments and opportunities in both the licit and illicit world for their activities. They act opportunistically and adapt accordingly.[43] For instance, criminal networks utilize new possibilities offered by digital platforms to come in contact with individuals who can carry out tasks or facilitate financial transactions. See paragraph 5.1.

There is a cat-and-mouse game between agile criminals and a reactive government.[44] For instance, criminal networks adapt their modus operandi in response to changes in laws and regulations or government intervention. There are indications, for example, that criminal networks smuggle cocaine in several small shipments and/or via several smaller ports instead of in a few large shipments via the larger ports, where there is more supervision and law enforcement. This is to reduce the risk of detection.[45]

Examples of the adaptive nature of criminal networks

Adapting to port measures:
"The strategies criminal organisations use to import their shipments of cocaine and extract them from the seaport are constantly changing, as criminals adapt to the measures implemented by the investigation services and (port) companies."[46] In the port of Rotterdam, a decrease in the quantity of cocaine seized was observed in 2024 compared to 2023. One explanation provided is that a displacement effect has occurred towards other ports due to the measures taken in Rotterdam (and Antwerp). At the same time, it is possible that not (only) the location has changed, but that the modus operandi or smuggling routes have been adapted.[47] The Research and Data Centre (WODC) stated in 2026 that due to increased security and control, the import of cocaine into the Netherlands can no longer take place without "inside help". This is evident from the criminal investigations examined by the WODC.[48]

Responding to anti-money laundering efforts:
During a meeting with anti-money laundering professionals in November 2025, a FIOD detective provided insight into the way criminals circumvent legislation and investigation. Anti-money laundering efforts ensure that criminals become 'enviably innovative'. As an example, he mentioned that "[...] Chinese students use criminal money to make luxury purchases in Europe, such as watches, jewellery, and perfumes. They then smuggle these to China, where they are sold at exorbitant prices. The proceeds flow back to the European clients, laundered via underground banking."[49]

Continued criminal activity from detention:
Continued criminal activity from detention (VCHD) also serves as an illustration of the agility of criminal networks. Although detained and/or convicted, kingpins can continue to run their criminal operations. This includes issuing assassination orders or managing their criminal enterprise. They have apparently accumulated such power and resources that they are not stopped by detention. They can continue to communicate in various ways, for example, via smuggled phones, visits or mail. Newer means of communication, including drones, can also be used for this purpose. While much attention is focused on the kingpins in detention, the periphery that enables VCHD is not fully understood. Consequently, the actual extent of the vulnerability to VCHD also remains unclear.[50]

Chemical camouflage of cocaine:
The agility of criminal networks is also evident from the shift toward the chemical camouflage of cocaine in various legal commodities, such as cocoa powder or fertilizers. By bonding drugs to other substances at a molecular level, they are not visible on scans, cannot be smelled by detection dogs, and colour tests do not react. This evolving method is accompanied by a rapid proliferation of specialized extraction labs and the international deployment of expertise.[51]

Box 2.3

3

Criminal networks use attractive and vulnerable infrastructures

Photo: Logistical hubs such as airports play an essential role in enabling criminal networks to achieve their objectives.

Criminal networks primarily use Dutch infrastructures for illegal gain. Derived from this, various (sub)objectives can be distinguished for which they use infrastructures:
1. *Supporting/continuing business operations.*
2. *Protecting and shielding operations and finances.*
3. *Maintaining or expanding power and reputation.*
4. *Maintaining or expanding network(s).*
5. *Acquiring and manipulating information.*
6. *Obtaining access to locations, resources, and official documents.*

These objectives can be realized through diverse activities. Conversely, a single type of activity often contributes to the realisation of one or more objectives.

Criminal networks potentially use all Dutch infrastructures that are also attractive to legal companies. In the STAN, a distinction is made between: economic, political-administrative, social, ecological and international infrastructures.

They use these separately and in conjunction to achieve their goals and through various (combinations of) activities.

Criminal networks exploit unique vulnerabilities of individual infrastructures, but certainly also more general ones.

Detailed system vulnerabilities are:
- *a Unintentional government facilitation.*
- *b Limitations in the approach to subversive crime.*
- *c Limitations in laws and regulations.*
- *d Normalisation of crime.*
- *e Reduced trust of citizens in government and in each other.*
- *f Vulnerabilities in business processes.*
- *g Complexity in controlling the misuse of dual-use sectors and resources.*
- *h Vulnerabilities for groups, neighbourhoods, and sectors.*

These each, on their own, but especially in combination, provide opportunities for organised crime.

3.1 Criminal networks use infrastructures in various ways to achieve their goals

3.1.1 Criminal networks have various sub-goals

The primary goal of criminal networks is to obtain money by producing products, trading, or providing services in an illegal manner (see paragraph 2.2). Derived from this, various (sub)objectives and activities can be distinguished to make this possible (see figure 3.1). The first three are described below.

Criminal networks, just like legal enterprises, have to run business operations. One objective is therefore the “supporting/continuing of business operations” (supporting business operations). Activities that contribute to this include, for example, the keeping and storage of commodities[52], such as the storage of narcotics in empty containers in depots. Additionally, the import, transit, and export of commodities, such as narcotics or fireworks, is a distinct activity.[53] Furthermore, criminal networks invest a part of their income in activities, such as transport[54], or in business assets.

Unlike legal enterprises, criminal enterprises must seek to overcome the obstacles of illegality (see section 2.2.3). Therefore, their objective is also the “protection and shielding of operations and finances” (shielding). Examples of this include the use of cover loads, shell companies, and crypto-communication tools to mask activities.[55] In addition, money laundering schemes are established and used to give the funds earned through illegal activities a seemingly legal origin.[56] Other strategies include the use of legal entities in a way that conceals improper use, for example through straw-men, seemingly correct administration, and complex corporate structures.[57]

Goals and activities of criminal networks

Primary goal: to obtain money illegally

Goals, subgoals and activities to achieve (sub)goals	
1. Supporting business operations Supporting/continuing (daily) business operations	• Offering an alternative option for (im)material goals of society • Storing and preserving goods • Purchasing goods • Investing • Importing, transiting, and exporting illegal goods to and from abroad • Producing illegal goods and services • Trading goods and services • Selling illegal goods and services (crime-as-a-service) • Processing payments
2. Shielding Protecting and shielding of operations and finances	• Adapting information (processes) • Corrupting • Creating and maintaining support from the local community • Using shielded communication / encrypting transactions • Investing • Establishing and using legal entities • Outsourcing • Sabotaging • Applying physical violence • Applying psychological violence • Spreading disinformation and rumours • Money laundering
3. Maintaining power Maintaining and expanding power and reputation	• Controlling/acquiring/expanding crime market • Corrupting • Creating and maintaining support from the local community • Displaying and advertising • Investing • Applying physical violence
4. Managing personnel Maintaining and expanding network(s)	• Establishing/expanding alliances • Involving others • Corrupting • Outsourcing • Applying physical violence • Applying psychological violence • Continuing criminal legacy
5. Acquiring information Acquiring and manipulating information	• Adapting information processes • Obtaining information from data trade(rs) • Corrupting • Infiltrating • Observing and surveilling of persons and processes • Applying physical violence • Applying psychological violence • Acquiring access to information (processes) digitally or physically
6. Acquiring access Acquiring access to locations, resources and official documents	• Corrupting • Infiltrating • Investing • Applying physical violence • Applying psychological violence • Forging/buying official documents

Figure 3.1

Criminal enterprises hold a position in illicit markets and in economic and social infrastructures at any given time. Just like legal enterprises, they want to maintain and/or expand these. A third goal is therefore the “maintaining or expanding of power and reputation” (maintaining power). In particular, the use of psychological or physical violence, as well as acquiring influence, are important activities to achieve this.

3.1.2 Objectives are to be achieved through diverse activities

Goals are not realized by a single activity alone, but through a variety of activities (see figure 3.1). Criminal networks are agile and do not put all their eggs in one basket. They seek the simplest and/or least risky way to achieve a goal. For example, they obtain information by corrupting individuals, infiltrating organisations, or by threatening with or applying psychological or physical violence. Research (see paragraph 4.2) shows that these activities are interchangeable, although corruption appears to be the most common and primarily to obtain information. The sub-goal “maintaining or expanding network(s)” can also be realized through various activities (see box 3.1).

Examples of “maintaining or expanding partnership(s)” (non-exhaustive)

Activity	Example
Involve others	Criminal networks make contact with young people via online games and offer them small tasks.[58]
Use of psychological violence	Criminals make young people from families with financial problems dependent on them by providing their families with money.[59]
Corrupt	Bribing a police officer to obtain investigative information.
Continuing and succeeding criminal legacy	Acting as a mentor for personnel (such as family members) to continue activities.[60]

Box 3.1

3.1.3 Activities can serve various purposes

Not only can one goal be achieved through various activities, but one type of activity can also serve various goals. In particular, corruption can contribute to five of the six goals in several ways (see box 3.2).

Infiltration and the use of psychological or physical violence are also frequently mentioned as means to achieve various objectives, with violence being used both within the criminal network itself and externally.[61] For example, criminal networks pressure employees of organisations to provide information (see objective 5). Additionally, criminal networks use violence to settle conflicts within the criminal milieu in order to maintain or expand their power and reputation[62] (see objective 3).

Objectives and examples of corruption

Objective	Practical example
Protecting and shielding operations and finances	Corrupting investigative officers to obtain substantive information to evade justice, supervision, or law enforcement.
Maintaining or expanding power and reputation	Corrupting local officials to exert influence on decision-making.
Maintaining or expanding network(s)	Corrupting transport employees to involve them in activities.
Acquiring and manipulating information	Corrupting public officials to obtain information about 'opponents'.
Gaining access to locations, resources and official documents	Corrupting Schiphol employees to gain access to secure areas.

Box 3.2

Various means-end relationships exist between individual activities. Although they can be analytically distinguished, in practice, they are by no means always separable. For example, the 'direct approach' of employees and asking whether someone wants to earn extra money, can be perceived as both corrupting and threatening. Activities can also be deployed simultaneously or sequentially. An example is a person who was previously corrupted and is later threatened when things do not proceed as desired (see paragraph 4.2.1).

3.2 Criminal networks use infrastructures that are attractive

Criminal networks use infrastructures that are attractive. Infrastructures are defined as the entirety of facilities that allow a country to function. The term 'infrastructure' is used in a broad sense, and in this context, one should explicitly not only think of physical infrastructures such as the road network. It also explicitly concerns broader economic, political-administrative, social, ecological, and international infrastructures, and both offline and online (see figure 3.2).

3.2.1 The Netherlands is attractive to organised crime

The attractive aspects of the Netherlands for legal businesses are also attractive to criminal enterprises. For instance, there are several factors that make the Netherlands an attractive place to establish operations, including logistic hubs such as Schiphol and the Port of Rotterdam. The Netherlands also has a good digital infrastructure with fast connections and high-quality internet exchange points and data centres. Additionally, the geographical location of the Netherlands is very favourable. The Netherlands is located on the coast, and every point in the country is just a few hours away from an international and open border with Belgium and Germany. Furthermore, most Dutch people are multilingual. Finally, there is generally a strong entrepreneurial culture in the Netherlands due to the high number of self-employed individuals and small and medium-sized enterprises and associated cultural values such as frugality and financial awareness. A study on the business climate for drug crime in the Netherlands shows that many factors can promote a positive business climate. This study also indicates that only limited knowledge is available regarding many of these factors.[63]

3.2.2 Criminal networks use infrastructures that are attractive for achieving objectives

Criminal networks use infrastructures that align with their goals and are attractive. Potentially, all infrastructures offer opportunities. Yet, it appears that some infrastructures align more logically with these goals than others. For example, logistical hubs such as ports. In this regard, large ports are more attractive than small ports for importing larger quantities of illegal commodities. This is because more products can simply be transported through a large port than through a small one. However, the choice for a large or small port will also depend on other factors, including vulnerabilities. As a result, smaller ports could still be preferred, for instance, if there are fewer opportunities for oversight.

Analytically, five types of infrastructures have been distinguished, including twenty specifications (see figure 3.2). Locations where concentrations of infrastructures occur are particularly attractive to criminal networks. The Netherlands has many such concentrations, including logistical hubs such as the mainports: Schiphol Airport, the ports of Rotterdam, the North Sea Canal area, the area Zeeland and West Brabant, and flower auctions/the ornamental horticulture sector. Furthermore, concentrations exist at and in smaller seaports and airports, and on Amsterdam's business district (Zuidas) within the financial and legal sector.

3.2.3 Economic infrastructures essential for achieving the goals of criminal networks

Economic infrastructures are essential for the realisation of all previously mentioned goals. Logistic hubs (and associated sectors) are frequently mentioned when it comes to subversive crime. These are locations within transport networks where various modes of transport converge, such as roads, railways, (air)ports, and waterways, in combination with related business activities. These hubs, both individually and collectively, play an essential role in the execution of activities, particularly regarding business operations.[64] Both larger and smaller seaports, as well as inland shipping and water-bound industrial estates, constitute a key link in the import, transit, and export of illegal commodities to and from abroad, such as drugs.[65] The same applies to airports and distribution centres.[66] When measures are taken to combat crime for one (type of) hub, they can continue their activities within another (type of) logistic hub.

Another economic infrastructure of great importance is the financial sector. This plays a major role primarily in shielding, including money laundering, but potentially also lends itself extremely well to obtaining information, such as obtaining financial or personally sensitive data on adversaries.

The trust sector also offers opportunities and is attractive. The trust sector is versatile for use in criminal activity. Trust companies can play a role in the inconspicuous spending of criminal assets, but also in hoarding criminal funds for perpetrators and siphoning or channelling them, or helping to generate them.[67]

Sectors that also stand out are the real estate sector and liberal professions.[68] Criminal networks use the real estate sector for various purposes. The real estate sector includes, among other things, holiday parks, homes, storage warehouses and other real estate. They use these as a front, a physical meeting place, or a production or storage site. Experts believe that the criminal exploitation of real estate is a cause for concern. Houses are reportedly being purchased in large numbers, with various criminals utilizing the same facilitator (such as a bookkeeper or real estate agent). Purchased homes can be used for, among other things, money laundering, mortgage fraud, and the facilitation of other criminal activities, including market manipulation and price gouging for legal buyers.[69] Liberal professions include the independent professionals who work with a high degree of autonomy, expertise, and professional ethics, such as notaries, accountants, real estate agents, bookkeepers, and lawyers. Precisely because of their knowledge, expertise, rights, and (confidentiality) obligation(s), they are attractive for involvement in criminal activities. They can (un) intentionally provide legitimacy to the activities and the assets acquired by criminal networks. This is due to, among other things, the social standing of these professions, the official documents they can provide, and the advice they can give. They form the link to legitimacy, and criminals are therefore dependent on them. Lawyers have a special position here because they are both a liberal professional and a crucial part of the rule of law.[70] Other sectors mentioned in relation to subversive crime include: hospitality, car dealers, souvenir shops, leasing companies[71] , and the luxury goods sector.

Criminals also make use of sectors that can be classified as social services, namely services that are (at least partially) organised and funded by the government to promote the well-being of citizens. The healthcare sector in particular stands out. Experts state that namely privatisation has led to the healthcare sector being attractive to and offering opportunities for criminals.[72] Healthcare, for example, has flexible forms of employment such as self-employed personnel or temporary contracts as a challenge. The sector can also

Types of infrastructures and examples thereof (non-exhaustive)

Infrastructures		
Economical infrastructures	• financial sector	including crypto, prepaid, FinTech
	• logistical hub	ports, airports, mainports
	• social, societal and cultural sector	semi-government, sport clubs when it comes to societal components, nature managers, cultural sector, care sector, etc.
	• real estate sector	real estate, buildings on farmyards, houses, storage sheds, etc.
	• luxury goods sector	gold, expensive watches, boats
	• liberal professions	lawyers, notaries, accountants, real estate agents, bookkeepers
	• digital platforms	social media platforms, gaming platforms, web shops, websites
	• other	transport companies, car dealers, lease companies, agricultural sector
Political-administrative infrastructures	• judicial power	
	• legislative power	
	• executive power	
	• media and journalism	
Social infrastructures	• local environment	neighbourhoods, business areas, holiday parcs
	• population groups	
	• social network	
	• care sector	
Ecological infrastructures	• milieu	living environment
	• nature	flora and fauna
International infrastructures	• infrastructures abroad	
	• safe havens	
	• differences in laws and regulations, practices and culture	

Figure 3.2

be used for recruiting new personnel in youth care and mental healthcare. It certainly cannot be ruled out that criminals will undertake subversive activities in similar sectors (see paragraph 7.2). Additionally, housing is also a part of social services.

Finally: across all sectors, the crucial role that legal entities play in organised crime is prominent. It is relatively easy to establish a legal entity in the Netherlands. Legal entities such as private limited companies (BVs) or foundations are essential and can be used to disguise or facilitate activities, or to provide a legitimate appearance. As a result, money laundering or fraud can be carried out more easily without immediately drawing attention. In this way, criminal networks can spread their risks and shield their identity, while simultaneously gaining access to financial systems, business contracts, and markets. Legal entities can be involved in activities either knowingly or unknowingly. Thus, criminals may deliberately establish legal entities, as mentioned above. Conversely, criminals may also make use of legal entities, such as transport companies, without them being aware of it.

3.2.4 Political-administrative infrastructures essential for achieving the goals of criminal networks

The political-administrative infrastructures consist of:

- The legislative power: the power that makes, establishes, and amends laws.
- The executive power: the power responsible for the implementation of laws and the day-to-day administration of the country. They implement policy and ensure that it is put into practice. Law enforcement agencies are also included here.
- The judicial power: the power that settles disputes and adjudicates.
- Media: Media have three democratic functions, namely an informative function (for politicians and citizens), a watchdog function regarding power (government and its institutions), and a forum function (giving expression to perspectives, interests, and ideas from society).[73]

The possible interaction between organised crime and political-administrative infrastructures takes place in several ways. As a logical consequence of the illegal nature of organised crime, shielding is essential. After all, the legislative, judicial, and executive powers constitute an 'enemy' by creating laws and regulations to combat organised crime and ensure law enforcement. Moreover, criminal networks benefit from a poorly functioning criminal justice chain and a low probability of detection and conviction, allowing them to continue their activities unpunished for longer and to build up assets and positions of power.[74] Furthermore, the media can bring matters to light that are not in the interest of criminals, or conversely, they can be beneficial, for example, when it comes to spreading disinformation about competitors or government officials.

The executive power has a monopoly on the provision of certain products and services, such as permits and identity documents. Criminals also have a need for these. Consequently, government officials constitute attractive targets.

3.2.5 Social infrastructures essential for realizing the goals of criminal networks

Social infrastructures also play an important role. For example, criminal networks utilize local environments, such as sports clubs or schools, to pursue their goals. Examples include maintaining or expanding power through local associations or recruiting 'personnel' at schools or football pitches. It also appears that specific population groups are attractive to use.[75] For instance, young adults are attractive to deploy as labourers (see paragraph 4.1). Groups that distance themselves from society in some way, including sovereign citizens, can also be attractive. Furthermore, criminals can make use of sectors that provide social services (see paragraph 3.2.3).

3.2.6 International infrastructures essential for achieving the goals of criminal networks

Organised crime is largely international and is not limited to national borders. The use of infrastructures in other countries is therefore also essential. Dutch criminal networks are also active in other European ports.[76] Some countries are attractive to criminal networks as safe havens for residing and/or continuing criminal activities or for investing in real estate. Tax havens are attractive for money laundering.[77]

Digital innovations, infrastructures, and cross-border financial systems enable criminal networks to manage operations remotely, minimize risks, and move assets abroad. As a result, they can operate from the jurisdictions with the most advantages. An additional advantage is that geopolitical tensions and power shifts result in reduced global cooperation with certain countries and a strengthening of the ties between (certain) states and criminal networks for strategic purposes (see paragraph 7.6).

illustration 'safe havens'

Criminals relocate to countries where residence, logistics, and law enforcement are favourable, or conversely, they leave when their stay becomes too risky or risks are lower elsewhere. For years, Dubai was used as a safe location. Since the extradition treaty with the United Arab Emirates has come into effect, the Emirates have been consistently extraditing suspects.[78] Consequently, Dubai is losing its appeal as a hideout, and criminals are leaving.

Morocco is emerging as an alternative. Suspects with a Moroccan background are moving to cities such as Tangier, Nador, and Marrakesh. The country does not extradite its own nationals. Many suspects have family ties and assets there. The Spanish Public Prosecution Service indicates that Morocco is therefore becoming a hub.[79]

Furthermore, the Costa del Sol remains a location where international groups congregate. In Marbella, murders, attempted murders, and kidnappings linked to criminal groups are on the rise.[80]

Box 3.3

3.3 Criminal networks exploit system vulnerabilities

Whether criminal networks actually use infrastructures depends not only on their attractiveness, but also on characteristics that make infrastructures vulnerable to use or general vulnerabilities in the Netherlands, referred to as 'system vulnerabilities'. Suppose such barriers have been erected in the large Port of Rotterdam that its use is no longer worthwhile or is too risky; although the Port of Rotterdam remains attractive (i.e., it still aligns well with the objectives), criminals will look for alternative infrastructures with weaker points (i.e., more or greater vulnerabilities).

System vulnerabilities can occur simultaneously or reinforce each other. It is impractical to describe all (potential) system vulnerabilities and mutual relationships for all conceivable infrastructures. In the documents summarized by the SKC, hundreds of system vulnerabilities have been identified. Some are effectively equivalent, while others focus on a specific infrastructure; still others are more overarching and have varying levels of abstraction. In this paragraph, only a few system vulnerabilities are described, namely those that were particularly striking during the analysis because they occurred frequently or were uniquely surprising (see figure 3.3).

3.3.1 System vulnerability: Unintended government facilitation

The study 'Unintended undermining' examined the unintended side effects of government action or omission regarding drug crime, referred to as 'government facilitation'. This is defined as "the action or omission of the government which unintentionally creates a breeding ground for organised drug crime". It concerns the unintended consequences of conscious policy choices where the government failed to adequately consider those consequences. The report mentions three types. A first type is when a specific policy or approach leads to shifts toward other phenomena (such as a ban on certain commodities and services), other locations (for example, other ports), or other policy domains, thereby creating a waterbed effect. A second type concerns the conscious weighing of interests within policy on organised (drug) crime or crime in general, but also between policy domains such as security, economy, housing, or health. A third type is when policy is created without taking the criminogenic effects into account at all, such as the privatisation or liberalisation of certain markets without monitoring potential crime risks.[81]

Overview system vulnerabilities

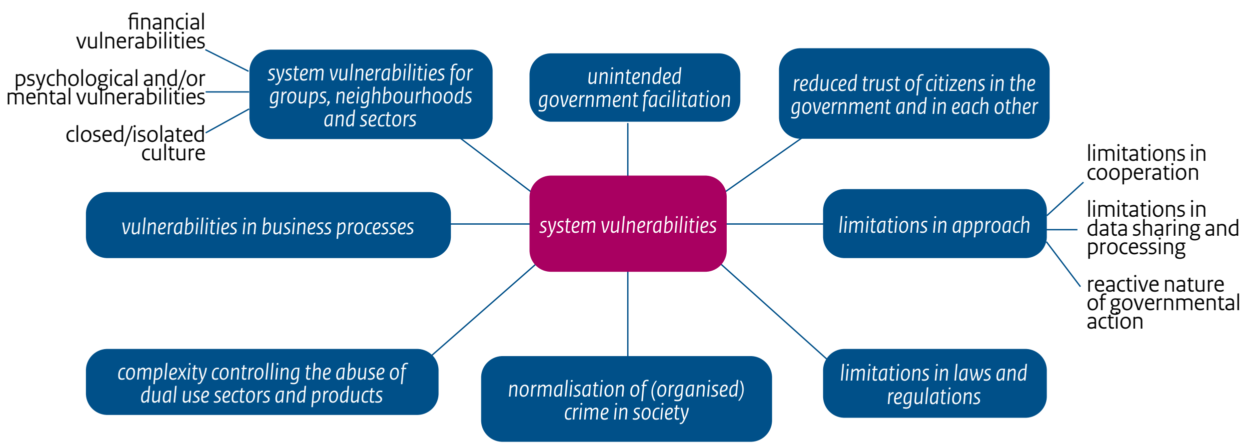


Figure 3.3

Although the research focused on drug crime, many of the findings correspond to a greater or lesser extent with findings in other reports and/or what was contributed during the expert meetings for the STAN. For example, several experts have indicated that law enforcement is at odds with other government interests, where law enforcement gets the short end of the stick.[82] For instance, over the past decades, much of policy has been aimed at stimulating and facilitating entrepreneurship, which has resulted in economic freedom being at odds with barriers against crime. Restrictive laws and regulations, such as the requirements to start a business, were removed or extensively relaxed. Consequently, the government has fewer instruments at its disposal to combat undesirable excesses and malicious practices. Criminals take advantage of this, and these excesses are becoming increasingly visible.[83]

Blind spots due to organisational goals

In an expert session, blind spots were discussed that arise from performance-oriented accountability within criminal prosecution. There is a focus on having a charge proven, but backgrounds - such as the way criminals obtained their money, their possible position of power, etc. - are not considered. The key performance indicators (KPIs), for example, are focused on numbers rather than a more system-oriented approach. Parties working together do not align their goals and KPIs. This approach primarily affects operatives, such as youth who are deployed for high-risk tasks (such as extractors and placing fireworks bombs at opponents), while the core of criminal networks remains intact. Attention is paid to the number of cases, seized assets, and the number of prosecutions.[84]

Box 3.4

3.3.2 System vulnerability: Limitations in approach

Limitations in cooperation

The approach to subversive crime requires cooperation between multiple public (and often also private) parties. This cooperation is often complex, as it operates interdepartmentally, intergovernmentally, and locally.[85] Additionally, it is far from always clear who the problem owner is and with whom shared responsibility must be assumed. Due to the fluid nature of subversive crime, it is difficult to determine who should be involved and what structure should be established for the approach.[86] The performance-oriented accountability of (government) organisations also plays a role. Furthermore, the mandate does not always align with the objectives of the organisations with which cooperation is undertaken.[87]

Although the focus on subversive crime has brought many benefits, the multi-interpretable term 'subversive crime' and the extensive discussion surrounding the utility of the term can also have a paralyzing effect at an operational level.[88] For example, several participants in the expert meetings felt that various interpretations, applications, and delimitations of the concept of 'subversive crime' lead to fragmented approaches that focus on incidents or individual cases rather than on the underlying problem.

Structural causes and core problems of data sharing

The Dutch Taskforce on data sharing identifies three structural causes of bottlenecks in data sharing:

1) Lack of implementation support, with the core problems being:

- Legal considerations are shifted to the operational level; professionals lack formal backing in complex cases.
- Executives receive conflicting internal advice and therefore operate under persistent legal uncertainty.
- Implementation support is fragmented, incomplete, or completely absent.
- There is no clear system or task responsibility that structurally supports cooperation.
- There is a lack of shared working methods, uniform agreements, and national frameworks for data sharing.
- A culture of risk avoidance prevails – fuelled by fear of personal liability, administrative disapproval, or simply the precautionary principle.

2) Lack of professionalism, professional community & knowledge management, with the following core problems:

- Insufficient legal, organisational, and functional expertise within organisations.
- The organisational embedding lacks ownership of data (sharing).
- No structural knowledge management or government-wide professional community.
- Lack of practical means such as formats, tools, and privacy enhancing technologies.
- Knowledge is tied to individuals and is lost when employees leave.
- Legalistic thinking is dominant; design-oriented, participatory approaches are given little room.

3) Lack of vision and anchoring, with the following core problems:

- There is a lack of a single overarching perspective on data sharing upon which policy, implementation, and legislation can build.
- Data sharing is insufficiently considered in the development of policy and legislation.
- Lack of a concrete toolkit for the policy officer regarding digital consequences, including data exchange.
- Expertise and structural support are lacking in policy and implementation structures.
- Responsibilities are fragmented; there is no clear, coherent governance providing direction.[89]

Box 3.5

Limitations in data sharing and processing

Data sharing is the digital extension of collaboration, and that makes it at least as complex, according to the Dutch Taskforce on data sharing (Taskforce gegevensdeling). The Taskforce stated in 2025 that in recent years "various reports, letters and initiatives have been issued that map out the bottlenecks surrounding data sharing within the government. These publications show that bottlenecks on organisational, technological and legal levels hinder the effective and careful exchange of data".[90] These barriers also emerged from the documents reviewed and the expert meetings held.

During expert meetings, several organisations spoke of a "culture of fear of making mistakes". The childcare benefits scandal (Toeslagenaffaire), which emerged in 2017, and its aftermath certainly play a role in this. This fear has a paralyzing effect within several organisations.[91]

Illustration of a culture of fear

Mayor Buma of the Dutch city Leeuwarden expressed, in an interview published on 3 December 2025, his views on the balance between, on the one hand, a government that must help vulnerable people and keep society safe and, on the other, compliance with rules. Although the interview does not specifically focus on subversive crime, what he said is also applicable to subversive crime. For instance, he stated that in isolation, facts may seem innocent, but taken together, they demonstrate that something is going on. He added: "And it is so strict, and the chance of mistakes is very high, especially with all the negative media attention. It almost seems as if the most important thing for the government is simply to stay within the lines. That is how you do it right. And whether an individual eventually falls through the cracks is almost less important than being able to say: 'At least we followed the rules correctly.'"[96]

Box 3.6

Illustration of the consequences of restrictions on data sharing

Trade based money laundering * (TBML) "... is challenging to detect and investigate. In an ideal situation, investigation services have access to transaction data, trade data, and financial data. However, no single private, supervisory, or investigation agency in the Netherlands possesses all of this data. Based on transaction data alone, it is difficult to substantiate a suspicion of TBML. For a successful approach to TBML, organisations will have to work together. This brings challenges, as it is not always possible to share information within existing legal frameworks. [....] There is therefore a high probability that any TBML schemes will go unnoticed."[97]

* Trade based money laundering (TBML) is a collective term for various techniques used to launder criminal proceeds through the use of international trade (Schmitz, Michael, 'Trade based money laundering: uitdagingen en ontwikkelingen binnen de opsporing', in Justitiële verkenningen Parallelle economie, jrg. 50, 2024, p. 78-105).

Box 3.7

Restrictions apply not only to data sharing, but also to data processing. For example, the Dutch Tax Administration used algorithms to detect abuse more effectively and in a more risk-oriented manner. The Dutch Data Protection Authority (AP) has expressed concerns about transparency and the risk of discrimination in the use of these algorithms. Here, the interests of privacy and law enforcement clash. Following the concerns of the AP, the use of several algorithms has been suspended.[92] As a result, the detection of abuse may be hindered.

As a result of the limitations in data sharing and/or processing, there is a fragmented picture of subversive crime. Moreover, subversive crime is a phenomenon that manifests broadly throughout society and criminal networks are agile. This has numerous consequences. It hinders cooperation in tackling subversive crime between public parties, between private parties, and between public and private parties. This plays into the hands of criminals: for example, they deliberately spread their activities across multiple banks, while banks are seldomly allowed to exchange data. Signals of criminal interference are not always recognized, for example within sports organisations, meaning that information that should be shared is sometimes not even detected.[93] In the report "Ondermijning op het platteland" (Subversive crime in rural areas) it is described how the Netherlands Police have hardly shared any more information with special investigating officers (BOAs; buitengewone opsporingsambtenaren) working in environmental enforcement since the General Data Protection Regulation (GDPR) come into force in 2018, leading to gaps in supervision and law enforcement. The GDPR does not apply to the investigative tasks of BOAs, as these fall under the Wet politiegegevens (Police Data Act). However, it is the GDPR, and not the Police Data Act, that is governing when police data is used for other purposes, such as carrying out the law enforcement task. In smaller and medium-sized municipalities with a rural character, this leads to issues relating to subversive crime becoming less visible.[94] Due to the lack of a comprehensive picture, illegal activities can continue, allowing criminal networks to expand further and remain (partially) under the radar of law enforcement agencies.[95]

Example of the reactive nature of laws and regulations

A participant in the expert session on the legal profession notes that the government does not always take the consequences of measures into account in its actions. The ban on lawyers taking laptops, mobile phones, tablets, or USB sticks into some penitentiary institutions is cited as an example. The measure was introduced to combat contraband and continued criminal activity by detainees. According to participants in the expert session on the legal profession, the measure is unworkable and far-reaching, and other smuggling methods remain unaddressed.[99]

Box 3.8

Reactive nature of government action

The often reactive nature of government action is at odds with the agility of criminal networks. For instance, intervention in the use of legal entities by criminals often only occurs once such abuse actually takes place. While indicators often already point to this intention, the Chamber of Commerce and, by extension, regulators or investigative authorities can often do little, even after a risk signal from Justis (Dutch screening authority that assesses the integrity of individuals and organisations) regarding potential abuse.[98] This reactive nature is also evident in the supervision of new, often digital, payment platforms. These develop so rapidly that effective supervision is often lacking and no clear picture of the abuse exists. Consequently, criminal networks can execute transactions and stay under the radar (see paragraph 7.5). Another dimension of this reactivity is that laws and regulations are often a response to incidents that occurred years earlier (see box 3.8). Furthermore, there is a risk that they focus on only a part of a broader problem, and other values or interests may be compromised.

Limitations in the approach to international aspects

The aforementioned challenges and vulnerabilities are also reflected in an international context. For instance, it appears that criminal networks can also take advantage of differences in laws and regulations between countries and the cumbersome information exchange that can arise between countries. Additionally, activities that cross national borders raise the question of who is responsible for what, such as who is leading the investigation.[100] As a result, criminals can remain under the radar for longer by exploiting the resulting delay.

3.3.3 System vulnerability: Limitations in laws and regulations

Regarding the complexity of laws and regulations, privacy legislation scored particularly high, especially with regard to data sharing. This complexity creates room for interpretation of the rules. Even within an organisation, different views may exist on how GDPR legislation can be interpreted. The combination with sectoral legislation, the difficult alignment with other legal regimes such as the Police Data Act, and the combination with professional confidentiality further increases the complexity. This complexity is reinforced by the fragmentation of organisations that must exchange data in order to collaborate effectively.

Other forms of complexity and gaps in laws and regulations have also been identified. An example is the Public Administration Probity Screening Act (Bibob act). In many administrative bodies, the Bibob act is applied to permits in the hospitality and construction sectors. In addition, the legislation can also be applied, among other things, to government contracts, such as public procurement in healthcare. Partly due to the complexity of this subject, it varies by administrative body whether the Bibob act is applied to these. In this regard, mayors are dependent, among other things, on expertise, capacity, and the willingness of the municipal government to cooperate. In small municipalities, the knowledge, skill, and capacity for this are often lacking. Criminals take advantage of this. Furthermore, the Bibob act is interpreted differently by each municipality: what one mayor allows, another does not. Another example concerns legislation on psychoactive substances (see box 3.9). Criminal networks structurally abuse complexity, loopholes, and gaps in laws and regulations, allowing them to operate relatively unhindered.

Example of gaps in laws and regulations and reactive nature

The fact that criminal networks strategically exploit legislative gaps is also evident in the trafficking of new psychoactive substances (NPS). Through minimal chemical modifications, these substances repeatedly evade existing criminalisation, meaning that investigation services had hardly any effective intervention options. While neighbouring countries already had specific NPS legislation, the Netherlands lagged behind, which led to its evolution into an international hub for the distribution of NPS.[101] To close this gap, since mid-2025, entire groups of substances with the same chemical base structure have been brought under the Dutch Opium Act, whereby a broad spectrum of common designer drugs was banned in one stroke.[102] Nevertheless, criminal networks still manage to identify and exploit new exceptions within these tightened regulations.[103]

Box 3.9

3.3.4 Normalisation of (organised) crime in society

A (potential) system vulnerability is the normalisation of crime in society. Experts differed in opinion as to whether this is actually the case. One topic that was discussed was the perception of widespread acceptance of drug use and dealing within Dutch society.[104] It is difficult to say whether, in absolute terms, there is a normalisation of drug use. The normalisation of drug use is a broad concept consisting of several components, including the availability and accessibility of drugs, the number of people who use drugs on a regular basis, social norms regarding drug use, and societal acceptance of drug use. Based on a definition of how many people use drugs on a regular basis or have used it recently, it can be stated that there is no normalisation in society as a whole. However, it is true that drug use is more normalized for some groups compared to other groups or relative to other years.[105] The National Drug Monitor shows that in 2024, 10.4% of adult Dutch citizens aged 18 and older used one or more types of drugs. This represents nearly 1.5 million adults. Among young adults aged 18-29, this percentage was higher, at 27.7%. The use of most drugs among adults in the Netherlands changed little in 2024 compared to the measurements from 2022/2023.[106] Furthermore, research shows “[....] that the use of alcohol and drugs is significantly higher among youth and young adults who go out than among peers in the general population.”[107]

There is a more nuanced view on whether normalisation is more widespread, for example, when it comes to turning a blind eye to crime or participating in it. It was argued that while taking money from other citizens is not acceptable, taking money from the government seems to be no problem.[108] This could be an explanation for so-called vertical fraud, such as the misuse of subsidy funds. Another observation is that a person does not necessarily become involved in organised crime due to changing norms and values. An individual’s personal circumstances, such as their financial position, can lower the barriers to becoming involved.[109]

3.3.5 Reduced trust of citizens in government and in each other

Reduced trust of citizens in the government and between citizens is a system vulnerability, because it can create a climate in which criminal networks can thrive. It can be accompanied by a decrease in the willingness to comply with rules or report wrongdoing, a decrease in the (normative) authority of the government[110], and a decrease in informal social control.

Research by the Netherlands Institute for Social Research (SCP) shows that citizens generally feel connected to the Netherlands and their neighbourhood and that there is mutual trust.[111] Conversely, citizens experience discrimination. In general, citizens have trust in the legitimacy of the Dutch government. However, trust in politics is relatively low. They also rate government performance relatively low on the points of responsiveness, procedural justice and its problem-solving capacity. Furthermore, these perceptions differ between groups in society, where, in broad terms, it can be stated that individuals in a relatively favourable position (such as sufficient income, education, and health) give a higher rating on these points than those in a more disadvantaged position (such as unemployment, experienced discrimination, and health problems).[112] Therefore, trust is unevenly distributed.

Furthermore, trust is not a static given. Trust in the government can fluctuate over the years and during major societal and economic issues, such as economic crises, the (approach to the) Covid-19 pandemic, and the (settlement of the) childcare benefits scandal (Toeslagenaffaire).[113] The degree of trust also differs between institutions. Recent CBS figures show that trust in other people has generally remained stable, while trust in institutions varies: executive institutions such as the Netherlands Police and judges are rated relatively high, civil servants score average, and trust in political institutions is lower, particularly in the House of Representatives and among individual politicians. Conversely, trust in local politics is higher.[114]

Diminished trust is certainly not only influenced by (the approach to) subversive crime. For instance, the government’s problem-solving capacity is generally perceived as low by citizens. Citizens experience a hardening of society and feel that groups of people are pitted against each other.[115] Diminished trust certainly applies to people who declare themselves sovereign: they distance themselves from the government and other institutions. Although they often maintain an open attitude toward other people, they do spread factually incorrect narratives about the malicious intentions of the institutions.[116]

Subversive crime erodes trust in the government and social cohesion (see sections 6.3 and 6.4), and thus contributes to a reduction in trust. This makes society vulnerable (or more vulnerable) to subversive crime, as described above. In this way, subversive crime creates a self-reinforcing mechanism between the system vulnerability ‘reduced trust’ and the subversive effects “erosion of trust in political-administrative infrastructures” and “erosion of social cohesion” (see section 6.7).

3.3.6 System vulnerabilities in business processes

Various factors and characteristics make business processes vulnerable to use by criminal networks. This applies at national, sectoral, and organisational levels. Identifying these requires extensive insight into specific business processes and specific organisations. Without claiming to be exhaustive, attention can at least be drawn to: a) vulnerabilities in 'employee processes', b) vulnerabilities in ICT and information processes, and c) vulnerabilities in the issuance process of documents that are crucial for criminal networks.

Various factors and characteristics make employee processes vulnerable to criminal networks. This is particularly true for a lack of screening of employees in positions that are crucial for criminal networks, for example due to their access to important information or locations. For instance, in 2024, the head of the Rotterdam seaport police pointed out vulnerabilities that arise when personnel in the port are not properly screened and trained.[117] According to the General Intelligence and Security Service (AIVD), the lack of screening within government organisations also constitutes a system vulnerability.[118] Vulnerability also arises when employees in key positions that are attractive to criminals can work autonomously without supervision by a manager or through digital monitoring (logs).[119]

Deficient authorisation, logging and monitoring and the insufficient implementation of basic cybersecurity measures constitute vulnerabilities in ICT and information processes. These constitute a system vulnerability in particular when it concerns information crucial to criminal networks, such as personal data, and/or where there is a concentration of information (processes). The head of the Rotterdam Seaport Police stated in 2024 that ICT within the international transport world is built to get a container to Europe quickly and at the lowest cost. The sector does not like complex authorisation models and logging[120], which lowers the barriers for abuse by (accomplices of) drug criminals. According to the AIVD, deficient logging within government systems and protective monitoring also constitute a system vulnerability.[121] Year after year, including in 2025, it is pointed out in the Cyber Security Assessment Netherlands (CSAN) that organisations have insufficiently implemented basic cybersecurity measures.[122]

Concentrations of information (processes) can be found in many organisations. In the CSAN 2023 and 2024, these concentrations are explicitly identified as a factor contributing to the persistent high level of digital threats. Concentrated information or processes are attractive targets for malicious actors and are therefore vulnerable to cyberattacks. If criminals manage to gain access, large volumes of information can fall into the wrong hands. CSAN 2025 notes, for example, that cybercriminals stole sensitive personal data and patient records from a laboratory affecting nearly one million individuals.[123]

Vulnerabilities also arise in the issuance of access passes and identity documents and the supervision of their authenticity. This is certainly the case for processes related to the issuance of documents that are crucial for criminal networks. Examples include the issuance and retrieval of access passes for (former) employees. There are also several vulnerabilities in the issuance process of identity documents.[124] Criminal networks want identity documents with which they can travel anonymously, and those vulnerabilities can contribute to this.

3.3.7 System vulnerability: controlling the abuse of dual-use sectors and products

Many sectors provide products and services that can be used for both legal and illegal purposes, the so-called dual-use sectors. Several legal sectors that are attractive for the realisation of the goals of criminal networks have already been discussed, including (but not limited to) the financial sector, the real estate sector and liberal professions.

At a lower level of abstraction, various vulnerabilities can be identified that contribute to use by criminal networks.[125] According to the AIVD, easy access to intelligence tools is an element that contributes to the development of high-quality intelligence capabilities of criminal networks. Spy shops play an essential role in this, but criminal networks also have access to technical spyware via regular online marketplaces. Vulnerabilities that can be distinguished in this regard are the absence of or gaps in the permit and/or registration requirement for purchase, limitations in the supervision thereof, and possibilities for anonymity of purchasers and cash payments. Another vulnerability identified by the AIVD is a lack of law enforcement of the permit requirement for private investigation agencies.[126]

In the CSAN 2024, it was stated that the scale and precision of the global trade in personally identifiable data can harm security interests. Various data companies trade worldwide in personally identifiable data of citizens and employees of organisations by offering advertisements on websites and apps. These companies build detailed personal profiles that are of great value to criminals.[127] For example, the location data of EU officials were obtainable from data brokers. As a result, these officials are susceptible to espionage, sabotage, and blackmail.[128] In addition, criminal networks can easily search for a great deal of information via the internet. There is still a lack of awareness among citizens and (employees of) organisations regarding the risks of sharing information when using social media.[129] The government also publishes a lot of information that may be relevant to criminal networks. This information is also susceptible to misuse by criminal networks.

Controlling the misuse of dual-use sectors and resources involves numerous complications. Measures to combat the misuse of these sectors and/or the products and services they provide by criminal networks are weighed against the bona fide use thereof. After all, these have consequences for the business operations of those sectors and/or for the government when it comes to, among other things, exercising supervision. Moreover, criminal networks are agile and can pivot to countries where these control measures do not apply or, alternatively, purchase resources online. Sometimes it is not possible or effective for solely the Netherlands to take measures, for example, when it comes to the use of social media.

3.3.8 System vulnerabilities for groups, neighbourhoods and sectors

A number of vulnerabilities can be considered at micro, meso, and macro levels. In the STAN, the emphasis is primarily on Dutch society as a whole or groups of people, neighbourhoods, and sectors.

Financial vulnerability

A common identified system vulnerability is 'financial vulnerability'. This applies, for example, to farmers who are facing uncertainty due to, among other things, the nitrogen policy and fishers who are affected by government measures. Also individuals such as migrant workers who are at or below the subsistence level may be susceptible to involvement. This is especially true if they are also employed in sectors that are crucial for organised crime, such as companies in the Port of Rotterdam or airport personnel.

Additionally, organisations that are in a sound financial position can also be vulnerable. The assumption that companies with a good financial reputation are less susceptible to government oversight likely plays a role in this.[131]

Police dog handler convicted for leaking information to criminals

In June 2025, a former police dog handler was convicted of leaking confidential information from police systems in exchange for payment. He was suspected of having accessed personal data and number plate information at least 42 times on behalf of criminals, possibly under duress due to threats. The Public Prosecution Service does not believe that the dog handler was coerced, but considers that he acted out of financial distress due to a gambling problem. According to the court, there is no evidence that he acted under pressure from criminals.[130]

Box 3.10

Psychological and/or mental vulnerabilities

Psychological and/or mental vulnerabilities among employees and directors of organisations, as well as citizens, can be exploited by criminal networks or contribute to involvement in organised crime. Examples include addiction issues, discrimination, bullying, adolescence, peer pressure, family problems, problems at school, psychological issues, people with a mild intellectual disability, and a desire for status or a luxurious lifestyle.[132]

Closed/isolated culture

Groups, organisations, or sectors in which the prevailing culture is one of closedness or isolation are more susceptible to the temptations of organised crime. This is evident, for example, in cultures of silence or cultures of tolerance. These cultures can be found both in the workplace and within subgroups in society. In a culture of silence or fear, people often do not feel free to discuss problems or raise misconduct. In a culture of tolerance, people know that something is not permitted or is wrong, but consciously overlook it or let it happen, leading to tacit acceptance. Additionally, the closed in-group culture has frequently emerged as a vulnerability. This culture has two sides: on the one hand, high social control helps prevent misconduct; on the other hand, people are less able to report misconduct and 'inform on' each other. Furthermore, internal supervision or control is less stringent because employees 'already know' one another. The analysis also identified cultures in which there is a taboo on asking for help. There are closed or isolated cultures in which locations are inaccessible or difficult for outsiders to enter, and professionals often have little insight into what is happening in these areas.[133] The baggage handling areas at Schiphol are mentioned in this context.[134] A cause for closed or isolated cultures is sometimes also found in a broader context, for example, among individuals who feel they have been treated unfairly by the government.[135]

3.3.9 Combinations of system vulnerabilities make infrastructures extra vulnerable

In practice, system vulnerabilities influence each other. For example, the involvement of youth in organised crime rarely arises from a single cause, but rather from an interplay of structural, social, and individual factors. Moreover, concentrations of vulnerabilities may emerge, for instance, in the case of digital platforms. These vulnerabilities can be used for many types of activities and can affect the mandates of many organisations. This can involve limitations in the approach to combat organised crime, as well as limitations in data sharing and data processing within and between organisations. Developments are moving extremely fast, while government action and laws and regulations do not always keep up with them.

4

The involvement of youth, and corruption, infiltration and violence

The involvement of youth, and corruption, infiltration, and the use of violence are frequently mentioned activities when it comes to subversive crime. The involvement of youth provides strategic added value for criminal networks. Involvement rarely arises through a tightly organised process and is not only initiated by criminals. This involvement not only has consequences for the young people themselves, but also for Dutch society as a whole.

The use of corruption, infiltration, and violence, collectively referred to as criminal interference, is increasingly necessary to sustain criminal business processes. Although the three activities can be analytically separated, they overlap in practice. Currently, obtaining information appears to be the primary objective of criminal interference, and corruption is by far the most common activity in this regard. Various vulnerabilities, circumstances, and societal developments play a role in criminal interference. Criminal interference has an eroding effect on the functioning of infrastructures.

The findings in this thematic chapter are based on insights from two recently conducted SKC thematic studies: “Youth” and “Criminal interference: corruption, threat and infiltration by organised crime in the Netherlands”. In both studies, depth was added via qualitative insights from interviews and expert sessions. This combined body of knowledge forms the starting point for this chapter. The involvement of youth is part of the threat “oil-effect of involvement in organised crime within society”(see section 7.3). Criminal interference is part of the threat “influencing decision-making and the functioning of institutions through structural manipulation by criminal networks” (see section 7.4).

4.1 The use of young people as labourers in organised crime

In line with the Preventie met Gezag program of the Government of the Netherlands*, the Thematic study on Youth focused on young people up to 27 years of age. This made it possible to draw on insights from a variety of sources and to justice to the complexity of youth recruitment into organised crime.

4.1.1 The use of young people is of strategic added value for criminal networks

Despite a structural decline in registered youth crime over the past 20 years, the problem remains concentrated within a relatively small group of young people. Within this group, there is a trend of hardening and an increasing rate of recidivism, with some progressing into organised crime. Criminal networks see strategic value in young people: they constitute cheap, flexible, and replaceable labour within an illegal economy that is constantly searching for new ‘personnel’. Furthermore, young people face lower legal risks upon arrest, enabling criminal networks to remain invisible by outsourcing high-risk tasks.

* a Dutch multi-agency programme aimed at preventing youth crime through coordinated efforts between municipalities, ministries, and social partners in designated high-risk areas

The appeal of young people lies in their combination of availability as labour and susceptibility to influence. Their knowledge of the neighbourhood, social networks, and ability to operate inconspicuously make them valuable for the local embedding of criminal networks. At the same time, their life stage increases their susceptibility to temptation and (peer) pressure. Because the brain is not yet fully development, young people are more sensitive to stimuli and short-term rewards, while limited future prospects for some youth may also strengthen the willingness to engage in risky behaviour. Criminal networks capitalize on this by offering money, recognition, and status. This creates a pattern in which young people are not only victims of influence but also become functional parts of criminal networks that benefit from their involvement. Their involvement thus reflects both personal vulnerability and a structural demand for operational forces within organised crime.

4.1.2 The involvement of young people rarely follows a structured process

The involvement of young people in organised crime rarely begins through a tightly organised process. It is primarily a combination of chance encounters, targeted approaches, and social influence. Young people are not only selected based on skills or availability, but gradually become entwined via existing networks in, for example, the neighbourhood, school, or sports environment. This subtle recruitment makes it difficult to gain control. Criminal networks exploit social and financial needs in this process. What begins with seemingly innocent odd jobs can evolve into structural involvement. Additionally, criminal networks - whether or not through family ties - strategically position young people within social sectors, for example, by directing them toward specific courses of study such as electrical engineering and finance, in order to deploy them later for criminal purposes, such as setting up cannabis plantations or managing financial flows. The boundary between voluntary participation and dependency blurs quickly, especially when pressure, loyalty, or the threat of violence comes into play. Young people experience a sense of agency but often operate within power dynamics in which others are in control.

Furthermore, recruitment is increasingly shifting to digital environments. Platforms such as Telegram and Snapchat facilitate large-scale and low-threshold recruitment by making offers to carry out 'odd jobs' in groups with tens of thousands of young people. Online networks reinforce physical contacts and make the dividing line between 'offline' and 'online' virtually meaningless. This interconnectedness increases the scale and speed with which youth can be reached and influenced, and creates a dynamic in which conscious and unconscious involvement merge seamlessly.

4.1.3 If support for youth is lacking, protective factors become risks

The involvement of young people in organised crime is rarely caused by a single factor, but by an interplay of structural, social, and individual factors. Young people growing up in environments with limited opportunities, low parental involvement, or unstable home situations run a higher risk of joining criminal networks. Personal circumstances, such as problems at school, associating with delinquent peers, or psychological issues, can also lower their resilience.

At the same time, vulnerability is not fixed. Factors such as social support, recognition of talents, future prospects, and a positive identity significantly reduce the likelihood of involvement. When young people feel seen and valued, their need to seek recognition in risky networks decreases. Notably, traits that are generally considered to strengthen resilience, such as intelligence, are used strategically by criminal networks. Thus, the same traits that make young people resilient can also increase their vulnerability when structural support is lacking. Vulnerability and resilience thus remain two sides of the same coin: support can mean the difference between being exploited by and being protected against criminal networks.

4.1.4 System vulnerabilities as a breeding ground for youth involvement

DESTEP developments reinforce each other in a way that makes young people more vulnerable to the influence of criminal networks. Behind individual choices lies a broader societal and institutional context of structural pressure: rising housing costs, pressure to perform in education, mental health issues and waiting lists for youth care create a context in which support structures are under pressure. As a result, young people experience less stability, while the blurring of norms and a growing fixation on financial success lower the social threshold for risky behaviour.

The digital space creates an additional layer of vulnerability. Online platforms influence behaviour, perceptions of status, and values. Young people are constantly confronted there with images of luxury, success, and making quick money. This constant comparison can heighten feelings of inadequacy or frustration and increase the appeal of alternative, including illegal, sources of income. At the same time, there is often a lack of professional oversight online, which limits detection and guidance. This creates a system in which social and digital vulnerabilities reinforce one another. The broader social context acts as a silent force behind the availability of young 'labourers' within organised crime.

4.1.5 High societal costs of youth pursuing quick money

Youth involvement in organised crime has consequences that extend beyond the individual. Participation in organised crime not only limits future opportunities and increases the likelihood of detention, violence, or addiction, but also puts families under emotional pressure, balancing between fear, helplessness, sadness, and shame. Victims and bystanders also experience physical and psychological harm, leading to increased feelings of insecurity and distrust.

At a societal level, this involvement undermines trust in institutions and social cohesion in some neighbourhoods. Visible threats, weapon possession, and online recruitment reinforce feelings of insecurity, especially in socio-economically vulnerable neighbourhoods where citizens feel that the government and the Netherlands Police are falling short. Although national figures indicate stable trust in the Netherlands Police and the justice system, accounts from the neighbourhood point to growing mistrust.

The tension between young people and adults is increasing. Young people are more quickly labelled as problematic, while older people, out of fear or mistrust, are becoming either more hesitant or more extreme in reporting incidents. As a result, conversations about norms and values are increasingly pushed into the background, partly because young people nowadays tend to form their worldview through (unfiltered) online sources. In this tension between insecurity, mistrust, and alienation, communities are becoming more vulnerable, in which youth involvement contributes to a creeping erosion of trust, safety, and solidarity - the foundations of societal resilience.

4.2 Criminal interference increasingly required for the continuation of criminal business processes

Criminal interference is increasingly often, or even always, a prerequisite for organised (drug) crime. Regarding criminal interference, criminal networks primarily use corruption. This is evident from interviews conducted with professionals from, among others, investigation and law enforcement.

4.2.1 Criminal interference has many faces

Criminal interference manifests itself through three activities*: corruption, threats and infiltration, in both public and private sectors. Although this threefold division provides analytical guidance, the activities frequently overlap in practice. For example, approaching employees directly, for instance by asking whether someone wants to earn extra money, can be experienced as both corrupting and threatening. Consequently, behaviours cannot always be unambiguously classified, and activities can be deployed simultaneously or sequentially. An example is a previously corrupted person who is later threatened when business does not proceed as desired. The boundary between corruption and infiltration is also blurred: interviewees cited cases in which individuals with malicious intentions applied for specific positions immediately after completing their education. Did they already intend to infiltrate during their education, or were they corrupted later?

* The thematic study uses the term "strategies" for this purpose.

Definitions from the Thematic study on Criminal Interference

Criminal interference: In the case of criminal interference, tasks of individuals, processes, and decisions within bonafide (government) organisations are disrupted by criminals. Actions, processes, and decisions are no longer (solely) carried out or made in the interest of the individual duties, the company, the organisation, or society, but in the interest of the activities of one or more criminal networks.

Corruption: "Abuse [...] of assigned powers or authority for personal gain."[136] Personal gain is also understood to include the avoidance of problems."[137]

Threat: "Threat refers to all forms of violence or aggression with which criminals attempt to influence (decision-making) processes. This does not only concern violence and aggression itself, but also the threat thereof. Examples of this include threatening telephone, email, or letter correspondence, physical threats, blackmail, and intimidation".[138] Threats to loved ones also fall under this.

Infiltration: "Any case in which a natural person who belongs to a criminal organisation or acts on behalf of a criminal organisation, or a previously infiltrated legal entity, invests financial and/or human resources to participate in the decision-making process of a legitimate company".[139] In this study, we exclude the financial component and focus on the strategic placement of persons within legitimate organisations.

Box 4.1

4.2.2 Full visibility of criminal interference is lacking

There is a lack of uniform and accessible registration of corruption, threats, and infiltration. A major reason for this is that these activities do not fully fall under specific criminal law provisions. For example, corruption is broader than bribery as described in the Dutch Criminal Code. Furthermore, the previously described variety of manifestations leads to diverging definitions, which complicates consistent registration. Where registrations do exist, as is partly the case with corruption, it is often not indicated whether a criminal network is the underlying actor, insofar as that is known at all.

4.2.3 Deployment of criminal interference depends on various factors

Criminal interference does not exist occur in isolation but rather supports the regular criminal business process. It is only when this process cannot continue without the assistance of employees within organisations that interference comes into play. Respondents from the environmental and healthcare sectors indicated that abuse of these systems is relatively easy, partly due to complex legislation. As a result, criminal networks can more easily stay under the radar, because understanding this complexity and thus being able to identify abuse requires specific knowledge, expertise, and capacity from regulators. These are frequently lacking. This makes interference less necessary for criminal networks. However, this does not rule out that interference occurs in these sectors. At the same time, criminal interference is primarily observed in organised drug crime. The professionals interviewed for this thematic study believe that criminal interference is increasingly, or even always, necessary to facilitate this. This is because combating it has led to increased supervision and barriers, meaning that help from within may actually be necessary to allow the criminal process to continue. The fact that creating barriers can actually result in a greater dependence on help from within was previously noted in the case of corruption related to drug crime in the Port of Rotterdam.

Obtaining information, particularly personal data and internal process information, currently seems to be the primary objective of criminal interference. In addition, criminal networks focus on resources, services, access, and evading oversight, as certain activities cannot be carried out by them directly. In this regard, individuals are specifically approached because of their position and workplace.

Corruption is by far the most common activity here. Threats occur primarily when a criminal network is under time pressure and no willing insider from the organisation is available, or when oversight must be diverted. Infiltration is rarely reported and is generally considered more likely in the private sector than in the public sector. However, respondents see shifts that can influence where and how interference occurs, at the level of location, organisation, function, smuggling method, and objective. For instance, the focus on combating corruption in the public sector may lead criminal networks to attempt to obtain personal data from information-intensive private sectors, such as insurers or mail-order companies. Measures can therefore create new shifts. Criminal networks continue to adapt relentlessly, and this also applies to criminal interference.

4.2.4 Systematic approach to criminal interference

Criminal interference, specifically corruption, has undergone a process of professionalisation. It can be described as a business-like approach. Previously, corruption was primarily related to pre-existing social relationships, such as friends and family. In recent years, corrupting individuals for information has increasingly been outsourced to information brokers. They have specialized in corruption and regularly maintain contacts with multiple corrupted employees to meet the information needs of criminal networks. They recruit via social media and other digital platforms. There are also brokers for managing support services. Another feature of the business-like approach, related to brokers, is the use of intelligence teams. Individuals who are attractive targets for corruption due to their position are tracked and screened, both offline (for example at sports clubs or catering establishments) and online via platforms such as LinkedIn, Facebook, and Instagram. In this way, criminal networks search for 'weak spots', such as debts or family problems, that make someone more susceptible to corruption.

4.2.5 Societal developments strengthen system vulnerabilities and vulnerabilities

Societal developments reinforce both system vulnerabilities and vulnerabilities at the micro level. Individual circumstances such as family problems, debts, a need for status, a luxurious lifestyle, or addiction increase the susceptibility to corruption. These factors often have a financial component, which is reinforced by rising costs and continuous social comparison in a digital environment. Technology also plays a dual role. New forms of monitoring, logging, and authorisation management in digital systems can improve detection and prevention, although these are often still in their infancy. At the same time, digitalisation and automation lead to more available data, making roles within public and private organisations more attractive to criminal networks. This may facilitate criminal interference or shift it toward digital activities, such as hacking.

Demographic, socio-cultural, and political-legal trends can also have an influence. Labour market shortages and an aging population can lower the quality of personnel screening, which facilitates infiltration and corruption. Additionally, a normalisation of crime and a hardening of society have been observed, which lowers the threshold for corruption and threats. Moreover, the 'tone at the top' plays a crucial role: when the leadership of an organisation does not prioritize criminal interference (whether consciously or unconsciously), there is a lack of urgency, policy, and support for vulnerable employees. Furthermore, this 'tone at the top' has a negative influence on the organisational culture. The interviews indicate that this culture also plays a part in whether or not criminal interference occurs. Finally, the new EU anti-corruption directive and other anti-interference initiatives may change the approach to and prevention of corruption, potentially with displacement effects in the longer term.

4.2.6 Criminal interference has an eroding effect on the functioning of infrastructures

Criminal interference has all kinds of subversive effects in both the public and private sectors, with consequences at micro, meso, and macro levels. These effects interact with one another, meaning that a single case can already cause significant harm. This can be illustrated as follows. Information or actions carried out by a corrupt official enable criminal networks to continue or optimize their business operations (indirect material). At the same time, individual task performance is affected (direct material) and the operation of the organisation is weakened (indirect material). Moreover, corruption can cause mistrust between colleagues and organisations (direct immaterial), which subsequently hinders further cooperation (indirect material). Citizens' trust in the government is also affected (direct immaterial), which reduces the willingness to report and cooperate, which is essential for the performance of public duties (indirect material).

Similar effects occur in cases of threats and infiltration and criminal interference in the private sector, where financial harm is usually more prominent. Public organisations also suffer harm, for example when information from an investigation is leaked. In a broader sense, criminal interference therefore has an eroding effect on vital infrastructures: it directly impairs functioning, thereby undermining trust in these infrastructures, which in turn further weakens functioning.

5

New opportunities for organised crime

Photo: According to experts, drones are transforming the way criminal networks are expected to operate in the future. See 5.1.2.

Developments in society influence subversive activities and system vulnerabilities and offer opportunities for organised crime. Developments that criminal networks can at least exploit to their advantage are:

- *Technological developments in unmanned systems (including drones), digital platforms, and Artificial Intelligence (AI).*
- *Geopolitical developments, such as the deployment of criminal networks by state actors, international sanctions and import tariffs, limitations in international cooperation, and the continuation or termination of Russia's war against Ukraine.*
- *Economic developments in digital payments.*
- *Social developments, including the desire to get rich quickly and prioritizing personal gratification.*
- *Ecological developments, including climate change, scarcity of raw materials, biodiversity loss and the energy transition.*

Demographic, economic, social, technological, ecological and political developments (DESTEP developments) fall outside the sphere of influence of criminal networks, but potentially offer opportunities due to their influence on subversive activities or system vulnerabilities. By analysing these developments, insights into these opportunities is gained, making the analysis more future-oriented.

This chapter addresses several technological, economic, social and ecological developments. No exhaustive research has been conducted into all conceivable developments that may be influential. The selection is based on sources reviewed, with some cases being validated in one or more expert meetings. The developments often do not have a clear boundary and influence one another.

5.1 Technological developments offer opportunities for organised crime

5.1.1 Continuous innovation and the global nature of digital platforms offer opportunities for organised crime

Digital platforms are now an integral part of daily life and are subject to constant change. A digital platform is an online environment in which users, providers, and systems can interact, communicate, or conduct transactions. These include, among others, social media, gaming platforms, digital payment services, and cryptocurrency providers.

Platforms are attractive to criminal networks for business operations, shielding, maintaining power, managing personnel, and obtaining information. An advantage is that they can operate efficiently, at scale, remotely, anonymously, and with greater security.[140] For example, they use social media platforms to recruit new (vulnerable) individuals in a low-threshold manner. For instance, a fifteen-year-old Dutch national stated that he had been recruited via Snapchat to shoot a Chechen mafia boss.[141] Criminal networks also use online games to offer jobs to potential recruits.[142] In addition, they use digital platforms to offer products. An example is the sale of drugs via Telegram or via the dark web. Some platforms, such as the aforementioned Snapchat or Telegram, or gaming platforms, are also used to communicate anonymously. The continuous innovation of digital platforms offers a virtually unlimited number of new possibilities.[143]

The approach to combat criminal networks that operate via digital platforms is complex. Due to the anonymity and concealment of identity, traceability to criminal networks is limited, making investigation more difficult. The approach also struggles with international jurisdictional issues, due to the scale and borderless nature of digital platforms, in combination with countries that each have different laws and procedures. Countermeasures or regulatory possibilities do not always keep up with the speed of developments. The government acts within established legal frameworks, while criminal networks are not constrained by these same rules and deliberately deviate from them.

Roblox as an example of a digital platform that is vulnerable to misuse by criminal networks

An example of a digital platform vulnerable to misuse by various malicious actors is Roblox. This is an online gaming platform where users create simple games and communicate with one another via avatars. The platform has approximately 150 million daily active users, more than 40 per cent of whom are under the age of 12. Due to its open design and chat functionality, young users can be approached and recruited with relative ease. Roblox also often functions as a gateway to external chat platforms where oversight is lacking and serious online exploitation can occur. In the Netherlands, the government announced an investigation into safety on the platform in October 2025. Roblox is attempting to address and curb this misuse.[155]

Box 5.1

5.1.2 Unmanned systems are transforming the criminal landscape

Unmanned systems, namely systems that can operate without human occupants, are developing rapidly and are increasingly being used. For example, self-driving taxis operate in the American city of San Francisco. In addition, drones are increasingly being used in warfare for laying mines or evacuating the wounded. In Russia's war against Ukraine, drones kill more soldiers and destroy more armoured vehicles than all traditional weapons combined.[144] Criminals will also be closely monitoring these developments.

According to experts, drones are bringing about a transformation in the way criminal networks will operate in the future. Drones reduce financial and operational risks for criminal networks, while expanding their tactical options.[145] The use of unmanned systems offers more flexibility to criminal networks and will reduce the risk of detection by law enforcement agencies and interception.[146]

Unmanned systems have various criminal applications and can be used on land, at sea, and in the air. In July 2025, an autonomously operated submarine with the capacity to transport cocaine was discovered in Colombia.[147] Criminal networks use unmanned systems for various activities, such as drug trafficking or smuggling contraband into detention facilities, as evidenced by a drone attempt to deliver drugs and a mobile phone to an inmate in De Schie in the Netherlands.[148] An English prison inspector warns of the possibility that, in the near future, a prisoner could be removed from a prison by so-called heavy lifting drones.[149] In addition to transport, small drones with a camera can be used as a means of espionage. In doing so, criminal networks can, for example, gather information from investigative agencies about ongoing criminal investigations. Additionally, they can be used counterstrategies, such as surveilling storage locations. Drones are also suitable for committing violence. For instance, in October 2025, individuals were arrested by the Belgian Federal Police one suspicion of planning a terrorist attack against the Belgian Prime Minister De Wever and a Belgian mayor. The police assume that the suspects wanted to attach an explosive to a home-made drone in order to carry out an attack.[150]

Intercepting criminal unmanned systems is complex. For example, drones can be small and quiet, making them difficult to detect. In addition, criminals are using increasingly sophisticated systems, causing government countermeasures to quickly become outdated.

5.1.3 Artificial Intelligence (AI) offers opportunities

AI is evolving rapidly and currently focuses on four important domains. Generative AI is developing quickly and is increasingly enabling the automatic generation of text, images, and audio. Within healthcare, AI is in full development and is progressively supporting the acceleration of drug development.[151] Semi-autonomous systems, such as self-driving vehicles and robots, are also further developing and are becoming increasingly independent in performing complex tasks. Additionally, AI continues to develop within business automation, where it makes processes such as data analysis more efficient.[152] However, the application and use of AI is not only of interest to society, but also to organised crime. For example, it can result in societal vulnerabilities or be exploited to achieve their own criminal objectives.

Criminal networks can utilize AI in various ways. Examples include its use for various forms of fraud, like the creation of deepfakes and phishing messages, the analysis of large datasets to identify potential targets, such as in stolen datasets, and the dissemination of disinformation. Additionally, AI can be used for the modelling and design of new chemical substances, which occurs in legitimate contexts within pharmaceutical research[153], but could theoretically also be misused for the development of new (synthetic) drugs. European law enforcement agencies, including Europol, warn that AI technologies in the hands of organised crime increase the scale, speed, and efficiency of digital crime, including online activities that facilitate drug and other illicit markets.[154]

Indirectly, AI can foster subversive crime when technological developments exacerbate societal vulnerabilities, such as labour market inequality, financial insecurity, or targeted online influence of vulnerable individuals through personalised messaging. In doing so, AI creates new opportunities for criminal activities on both a technical and social level. At the same time, AI can also be deployed to combat subversive crime, although this application is subject to strict preconditions and raises several questions.

5.2 Geopolitical developments present opportunities

Geopolitical developments refer to changes in global power dynamics, strategic positions, and political interactions between countries and regions. These arise from the interaction between geographical factors (such as location, raw materials, infrastructure, and territory) and political factors (such as power, policy, diplomacy, economy, and security). These developments influence Dutch society, including its vulnerabilities, as well as the actions of criminal networks, thereby exacerbating threats.

5.2.1 Global power shifts and change in global relations

Developments in strategic rivalry between great powers increase political tensions worldwide and thereby influence opportunities for criminal networks. The unipolar world system and the liberal international order are under pressure, weakened by the actions of great powers and the rise of new strategic powers.[156] Criminal networks can, for example, benefit from the focus on defence instead of organised crime, deteriorated diplomatic relations between countries, or internal political instability.

5.2.2 Criminal networks as part of hybrid warfare

Geopolitical developments are leading, among other things, to an increasing use of hybrid means for warfare by state actors.* Examples include the dissemination of disinformation, carrying out cyberattacks, the creation of unrest, or carrying out covert operations.[157] For this purpose, states deploy criminal networks as an 'instrument' in their hybrid toolkit to achieve geopolitical goals. Although the nature of hybrid conflicts remains the same, these hybrid means are being deployed more broadly, in a more targeted manner, and more aggressively.[158]

* A form of conflict between states, largely below the legal threshold of open armed conflict, involving the integrated use of instruments and actors to achieve specific strategic objectives ('De Veiligheidsstrategie voor het Koninkrijk der Nederlanden', 3-4-2023).

5.2.3 International sanctions offer opportunities

In the context of geopolitical tensions, international sanctions are applied to countries, and countries also impose import tariffs on one another. Existing smuggling routes used by criminals can be useful for circumventing sanctions. This can go both ways: from and to the country subject to sanctions. Due to import tariffs, trade routes may change, or trade to and from certain countries may increase or decrease. This also presents opportunities for organised crime. On one hand, they can 'piggyback' on intensified trade flows for illegal commodities. On the other hand, they can play a role in the smuggling of commodities and thereby evade import tariffs.

5.2.4 Reduction or termination of the war against Ukraine offers opportunities

Ukraine has developed a practical, operational foundation in the field of digital defence and cyber warfare. Upon the reduction or termination of the war against Ukraine, this experience and knowledge may become available to criminal networks. This experience and knowledge could enable them to further professionalize and strengthen their digital capabilities. Since 2014, with the annexation of Crimea and the start of the conflict in Donbas, Ukraine has repeatedly been the target of cyberattacks on banks, energy companies, and infrastructure. This has forced the country to set up cybersecurity centres and develop specialized teams. As a result, Ukraine has built up knowledge in malware analysis, DDoS protection, and the security of (industrial) systems. These are continuously applied and expanded in the current war.[159]

At the same time, the return of Ukrainian fighters, together with a surplus of weapons, ammunition and drones, can offer new opportunities for criminal networks. Returning fighters possess military training, logistical experience and knowledge of weapon systems, cyber systems and cyber-attacks, making them attractive for illegal trade, security services or paramilitary activities. According to the UNODC, the war has significantly increased the availability of weapons within Ukraine, as large quantities of military equipment can reach the civilian circuit. In the event of reduced intensity of the war, this knowledge, these surpluses and experienced returning fighters could lead to the expansion of the black market, new trade networks and a possible increase in violence and involvement in organised crime, such as through illegal arms trafficking or cybercrime.[160]

5.2.5 International cooperation under pressure

Geopolitical developments are influencing the international legal order and the legitimacy of multilateral institutions. Examples of this include the resistance to the United Nations and the International Court of Justice.[161] These developments also have an impact on a joint international approach to organised crime, such as international cooperation. Criminals can shift their activities to countries with less oversight or make use of logistics routes where oversight has diminished. For instance, following the outbreak of Russia's war against Ukraine, cooperation with investigative authorities in Russia to tackle cybercriminals is hardly possible. As long as Russian cybercriminals do not take any action against Russia, they can largely operate freely within Russia.

5.3 Economic developments offer opportunities

Economic developments refer to changes in the global economy (trade, production, prosperity, etc.). An important economic development is the ongoing digitalisation of the global financial infrastructure. Global payment systems have already been extensively digitalised, but this process is far from complete. Related services, supervision, and the global financial system (payments, banking, trade, identification, supervision) increasingly operate using digital technology instead of physical or manual systems. Examples include global cloud-based financial systems, digital identity verification of individuals, or AI-driven supervision and security.[162]

Another development is the further rise, growth and societal acceptance of digital currencies. Cryptocurrencies, digital money secured with cryptography that operates without a central bank or government as an intermediary, have become a structural part of the financial system in recent years.[163] Stablecoins are also increasingly being developed, a form of cryptocurrency with a relatively stable value, to combine the advantages of crypto with reduced price volatility.[164] See further section 7.5.

Another development is that of growing materialism and instant gratification. In Western societies, culture and consumption habits are shifting increasingly toward individualistic interests of 'quick money' or 'quick consumption'. This is also reflected via digital platforms such as social media, where users frequently showcase a luxurious lifestyle or commodities.[165]

5.4 Social developments offer opportunities

Social developments are changes in society regarding how people interact with one another, how groups in society develop, and which norms, values, and customs apply. This creates new opportunities for criminal networks to capitalize on.

Global inequality continues to increase, which not only widens the gap between rich and poor, but also worsens the vulnerable position of the poor. This trend is also visible in the Netherlands and is expected to continue. This naturally has consequences on political, economic, and socio-societal levels, such as access to social services and the lack of opportunities. For instance, shortages in the housing and labour markets may increase. This can result in declining trust and the disengagement of groups in the population.[166]

Additionally, democratic norms worldwide are under pressure, which also has consequences for the intensification of affective polarisation*. Themes with far-reaching consequences for society will (continue to) be addressed in the Netherlands, such as the energy transition, social security, the labour and housing markets, immigration, and healthcare. These themes contribute to increasingly extreme differences between groups, which can lead to further feelings of tension based on the 'us-versus-them' principle. Digitalisation, the use of AI, and disinformation mean that 'group viewpoints' can be shared and manipulated more quickly. The mutual alienation, discrimination, and lack of understanding between groups that can arise as a result go hand in hand with an increasing loss of trust in institutions.

* Affective polarisation refers to the extent to which groups not only disagree on substantive issues, but also develop strong negative feelings and mutual antipathy towards members of other political or societal groups.

Formal societal ties, such as associations, family bonds, and religious communities, have declined. As a result, people are increasingly seeking connection in informal groups with similar social, cultural, or economic backgrounds, which increases the likelihood of bubble formation. These informal networks often emerge outside traditional structures, such as sports associations or religious organisations, and have little to no oversight. Examples of this include informal sports activities or online spaces where young people gather, such as parts of the manosphere.[167]

Collectively, these developments increase the instability and vulnerability of society, which criminal networks can increasingly exploit. For example, socially or financially vulnerable citizens are easily approached, or disinformation campaigns are carried out to manipulate (groups of) citizens. Groups in which bubble formation occurs and who have a lower socio-economic status are particularly attractive for criminal networks to approach. Social discontent creates a breeding ground for citizens and organisations to procure services from criminal networks. Additionally, the aforementioned scarcities and tensions give rise to new lucrative markets to exploit.[168]

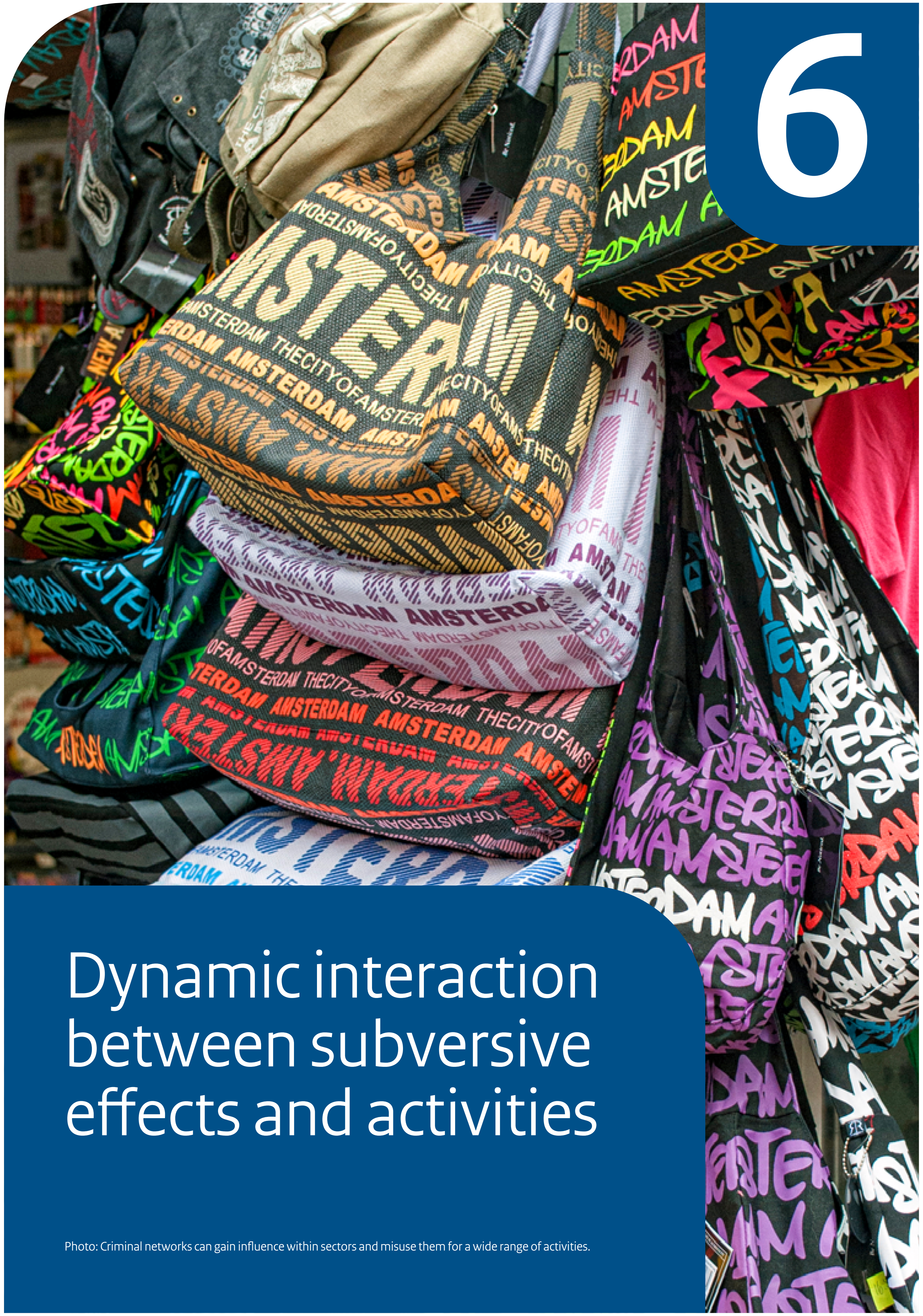
5.5 Ecological developments offer opportunities

Climate change, scarcity of raw materials, loss of biodiversity, and the energy transition are causing a structural reorganisation of economic and societal systems.[169] These ecological or related developments increase dependencies and create opportunities for criminal networks.

Climate change and extreme weather conditions, such as flooding, drought, and heatwaves, combined with water shortages and rising raw material prices, increase socio-economic risks for businesses and citizens in the Netherlands.[170] Financial damage, higher insurance costs, and societal tensions over climate measures increase the vulnerability of (groups of) citizens. Additionally, these circumstances can influence migration flows toward the Netherlands. Criminal networks can exploit this by offering illegal commodities and services or by exploiting vulnerable persons. Furthermore, the potential trade in specific rights, including emission-related rights, as well as subsidies for certain climate measures, offer opportunities for misuse.

Measures to protect the climate or environment sometimes lead to fierce debates between proponents and opponents. Air and water pollution and chemical or plastic pollution increase health risks and heighten societal concern.[171] This intensifies public pressure on governments and can erode trust in government agencies. In this context, opportunities arise for criminal networks to capitalize on the diminished trust of society and vulnerable groups.

The energy transition, electricity grid connection constraints, and the emergence of new markets for renewable energy, battery production, and critical minerals are leading to new dependencies and market shifts. As a result, new economic opportunities arise, but it can also result in vulnerable companies. Criminal networks can profit from this, for example, by abusing green energy projects.[172]



6

Dynamic interaction between subversive effects and activities

Photo: Criminal networks can gain influence within sectors and misuse them for a wide range of activities.

Subversive effects are the result of subversive activities. Combinations of subversive activities that, both individually and collectively, lead to economic, political-administrative and social harm are:

- *Criminal networks meeting societal needs.*
- *Recruitment and deployment of citizens, officials within specific professional groups and (employees of) organisations.*
- *Manipulation through various activities or as a side effect of activities, including the use of violence or via influence and a position of power in sectors or areas.*
- *Integration of illegal proceeds into society.*

Ecological harm primarily arises as a side effect of business operations, including the dumping of chemical waste, the release of harmful substances, or through explosions.

Harm to the international reputation of the Netherlands is linked to subversive activities abroad by criminal networks operating from the Netherlands. Harm also arises when the Netherlands is internationally regarded as a country that plays a significant role in organised crime and/or that has insufficient control over it.

6.1 Subversive effects: latent and dynamic

Subversive activities gradually and insidiously generate subversive effects in Dutch society, also referred to as harm or damage. First, these effects often do not manifest directly, but develop over time. For example, it can be argued that every individual case of corruption within the government is one too many. However, this does not directly lead to harm to society as a whole, but may result in harm to an organisation, or within a neighbourhood or community. If, on the other hand, corruption occurs frequently or for a long period, or takes on structural forms, it does indeed leads to harm to society as a whole. Secondly, there are poorly visible or even invisible activities, such as the dumping of chemical waste into the sewer system. Consequently, subversive effects, particularly in their initial phase, are not directly visible or noticeable. A third reason is that various subversive activities can lead to the same types of harm and thereby reinforce each other. This is because harm does not necessarily arise from individual subversive activities, but rather from the combination of activities. If subversive activities cumulatively lead to harm to society, this is difficult to reverse (see also section 6.7).

Harm arises from diverse subversive activities and, conversely, subversive activities can result in various types of harm. As a result, many relationships can be distinguished. Which effect occurs depends on the infrastructure affected, the type of activity, and also the underlying goal of criminal networks. After all, corrupting supervisory authorities responsible for legal entities for purposes of concealment has different effects than corrupting port employees for operational purposes. Furthermore, a single subversive activity has multiple effects. For example, corrupting supervisory authorities not only leads to harm to the vitality of and trust in political-administrative infrastructures. It can also lead to economic harm when bona fide entrepreneurs experience competitive disadvantages. Moreover, these relationships are dynamic and can vary over time. After all, criminal networks are agile and respond to, among other things, government interventions. These can lead to shifts in activities and/or used infrastructures and therefore also influence subversive effects.

An additional complication in this regard is that effects and the relationship with activities often cannot be determined objectively or empirically. After all, criminal networks have an interest in keeping their activities unnoticed. For example, they may try to hide illegal commodities among legal commodities, without the legal entrepreneurs being aware of it, or rent a car for illegal transport. What, then, is the harm to the entrepreneurs and society? This depends on many factors and is difficult to measure. Moreover, it is not always in the interest of the parties involved to register and share such incidents, or this may not be permitted by, for example, privacy legislation. To nonetheless provide insight into subversive effects, combinations of subversive activities have been chosen.

Five types of harm are distinguished: economic, political-administrative, social and ecological harm, and harm to the international reputation of the Netherlands. These types of harm align with the classification of infrastructures and the level of abstraction.

6.2 Economic harm due to subversive activities

Subversive activities lead to economic harm because they affect the vitality of and the trust in economic infrastructures. Vitality refers to their sustained functioning. This involves, for example, disruption of the financial sector and payment systems through the mixing of legal and illegal assets, and the weakening of legitimate sectors through unfair competition and tax evasion. It also concerns the declining quality and attractiveness of local economies due to the neglect or displacement of regular businesses, rising rents, and vacancies. Trust relates to the extent to which citizens and entrepreneurs believe that economic infrastructures are fair and reliable. An example of the erosion of trust is a diminished sense of justice among entrepreneurs because malicious practices (seem to) pay off and the government does not intervene effectively.

The assumption in this STAN is that economic harm primarily arises from the intertwining of illegal and legal activities within economic infrastructures in the Netherlands, whereby the boundaries between legal and illegal activities are to a greater or lesser extent. This intertwining has been operationalised as:

- Integration of illegal proceeds into society.
- Recruitment and deployment of - originally - legal market parties in subversive activities.
- Manipulation of economic processes through various activities.
- Criminal networks meeting societal needs.

Illegal proceeds find their way into society through criminal networks that launder these proceeds and invest them, for example, in legal entities and/or misuse various financial channels. This disrupts the vitality of economic infrastructures because markets no longer function fairly. Staff can be paid with criminal money[173], distressed companies can be kept afloat, or real estate can be acquired with illegal funds[174] that would likely not have accessible without criminal proceeds. Because illicit enterprises derive their income from other sources, they are, for example, less affected by high rents or a lack of customer footfall. Moreover, paying staff off the books, skimming off turnover, and the sale of illegal commodities can also contribute to a more favourable position for illicit enterprises compared to legitimate enterprises.[175] Economic activity is thus no longer guided solely by economic principles, such as supply, demand, and productivity. Ultimately, the economy becomes less efficient, less productive, and less stable, all the more so when this mixing and these mechanisms persist over time.

In the long term, intertwining can also lead to the undermining of public trust in the economy and to a diminished sense of justice among entrepreneurs. For example, entrepreneurs in the Amsterdam city centre, among others, are concerned about increasing shop rents and the disappearance of retail offerings. Additionally, it discourages compliance with rules. Bonafide entrepreneurs in the city centre of Amsterdam feel that criminally funded companies have an advantage, which affects the sense of justice and could potentially also lead to a shift in the perception of norms[176] (see also box 6.2), mistrust, and cynicism. Bonafide companies become wary of establishing themselves in sectors or neighbourhoods where criminals call the shots. Moreover, a self-reinforcing mechanism can emerge. Enforcing the law, for example, becomes increasingly difficult due to the blurring of the line between legal and illegal, combined with complex international structures and front companies behind which criminals often hide. Criminal networks can benefit from this in turn. In the long term, a self-reinforcing spiral can thus emerge: criminal behaviour weakens the sense of justice and public trust, thereby increasing the likelihood of further intertwining.

Company used for laundering assets
A drug trafficker spent nearly €3.5 million more between 2017 and 2021 than he legally earned through his car dealership or other work. The District Court in Den Bosch (The Netherlands) concluded that this money must have originated from drug trafficking and sentenced the individual to eight years in prison. The at least €3.4 million he earned from drug trafficking was subsequently invested for years in a car business run by a father and son. For unclear reasons, the car business had been in severe financial difficulty for years prior to this.[177]

Box 6.1

Example of feelings of inequality before the law
According to a 2024 study, entrepreneurs in the Amsterdam city centre experience that shady or possibly fraudulent shops continue to exist, while bona fide entrepreneurs are strictly inspected for minor violations. This leads to feelings of legal inequality and, as one entrepreneur stated, undermines trust in the government. At the same time, it creates an environment in which the crossing of norms is normalized. The entrepreneurs fear that this negatively affects the bona fide business climate. [178]

Box 6.2

Another cause of economic harm can stem from the involvement of (employees of) companies in subversive activities. Although this does not always involve coercion, it does occur in some cases and affects the safety of employees. As a result, positions that acquire a certain degree of notoriety may be perceived as less attractive.

Company used for laundering criminal money
In February 2026, the OM announced in a press release that it had imposed a €500,000 penalty order on a company for violations of the Dutch Anti-Money Laundering and Counter-Terrorist Financing Act (Wet ter voorkoming van witwassen en financieren van terrorisme, Wwft). "The company failed for a prolonged period to adequately verify the identity of customers who repeatedly spent large amounts of cash. The OM is disposing of the case through a penalty order in order to free up scarce court capacity at the District Court of Rotterdam (The Netherlands). The money laundering case originates from proceedings against a now-convicted underground banker who collected large sums of criminal proceeds in criminal circles to launder them." The suspect spent this money under various names on luxury goods. The bags were then sent by the suspect to China to be resold there. "In this way, the proceeds appeared to originate from legitimate trade. This is known as 'Daigou' trade and is a method of moving criminal funds through luxury goods." In addition to the buyer, two other suspects have been identified in the money laundering case. One of them is a former sales employee of the company. The proceedings against the three suspects were still ongoing in February 2026. [179]

Box 6.3

"Port companies and transporters can unintentionally become involved in cocaine trafficking and expect misery. The fear experienced in the port is quite profound. [...] Violence and intimidation; tracking down employees at home, in the café, or at the gym; infiltration, recruitment practices, hundreds of extractors on the premises whom you, as an employee, may encounter: the high-risk companies have all had experience with this."[180]

6.4 Risks for port companies and transporters

In the long run, criminal networks may gain influence over or build a position of power in sectors and/or neighbourhoods through ownership of or control over, for example, real estate, hospitality establishments, or companies in logistics sectors. This enables them to manipulate economic decision-making and the functioning of institutions. Tops and Van Der Torre mention various economic roles that criminals can fulfil, such as:

a) a client in legal sectors by providing work to, for example, automotive businesses.

b) an employer of, for example, migrant workers.

c) a housing provider for vulnerable groups.

d) a banker for entrepreneurs or people with debts.[181]

There are no indications that criminal networks have an economic sector or location under their grip, but there are indications that they exploit them. This can give criminal networks more economic power. For instance, they make use of existing (logistics) chains of legitimate companies, establish legal enterprises (using a front person)[182] to carry out or conceal their activities[183], and invest their acquired assets in the legal economy by, for example, purchasing (local) real estate.[184]

Economic weight in holiday parks
An example of the economic power of criminal networks is visible within holiday parks. Criminal networks can acquire influence in a holiday park by investing in it, buying shares, or providing a loan. In this way, criminal networks bear none of the costs (responsibility for operations or debts), but do receive the benefits (control over the distribution of profits).[185] Furthermore, holiday homes can be used for criminal activities such as drug production or prostitution, but also for forms of housing that violate laws and regulations, such as the illegal housing of migrant workers or persons without a right of residence.

When criminal networks have influence in holiday parks, other investors may become reluctant to invest in those holiday parks. This can create a negative spiral between vitality and trust.

Box 6.5

6.3 Political-administrative harm due to subversive activities

Subversive activities lead to political-administrative harm because they undermine the vitality of and trust in political-administrative infrastructures. Political-administrative infrastructures are broadly defined and encompass the judiciary, legislative and executive powers, as well as the media (see paragraph 3.2.4). Vitality refers to the intended functioning of these infrastructures. Harm may arise if, for example, there is: undermining of the independence of the judiciary, conflicts of interest among administrators, threats to journalists, undermining of the functioning of political representation, undermining of the functioning of public administration and the civil servants associated with it, undermining of the security apparatus, and loss of the government's monopoly on the use of force. Trust concerns the faith that citizens have in the fairness, reliability, and legitimacy of political-administrative infrastructures.

When referring to political-administrative harm, the assumption in this STAN is that it primarily stems from: *

1. Manipulation through:
   a) shielding, allowing criminal networks to remain under the radar,
   b) active opposition to the rule of law and
   c) influence and/or position of power.

2. Recruitment and deployment of officials and employees.

3. Criminal networks meeting societal needs.

* The extent to which government institutions are capable of curbing organised crime also plays a role in the harm that may arise. This latter perspective is, within the DON, considered part of systemic vulnerabilities and is not further elaborated on in this chapter.

Due to the illegal nature of criminal networks, shielding operations and finances is necessary. To stay under the radar, criminal networks employ all kinds of defensive counterstrategies (see section 3.1.1). The length of time that criminal networks are able to persist contributes to the threat they pose. According to Europol, 34% of criminal networks have been active for more than 10 years and are able to maintain their influence and power.[186] Through access to encrypted communications between criminals, criminal networks were detected that otherwise could have continued for years. When criminal networks can successfully operate under the radar without the government being able to intervene effectively, trust in the rule of law erodes.

Criminal networks also employ offensive counterstrategies and, especially when their interests are under pressure, actively challenge the rule of law (see section 7.4). The vitality of and trust in the rule of law are undermined when criminal networks actively challenge the rule of law. In such a situation, fear can play a role in decision-making and the functioning of institutions. This undermines the foundation of the democratic rule of law: a system in which an independent judiciary, transparent provision of information, and integral institutions form the basis for legitimate decision-making and societal stability. Citizens and companies lose confidence in the government when the integrity of civil servants is at stake. Furthermore, officials within the rule of law may become cynical or experience feelings of powerlessness.

Impairment of the functioning of the rule of law by threats of violence from criminal networks
A 2023 survey by Investico and De Groene Amsterdammer among Dutch judges and prosecutors shows that half of them have encountered threats in their work, often originating from the criminal world. In a third of the cases, these concerned matters of organised crime, such as the Marengo trial. Threat and violence lead magistrates to adjust their work practices: some dossiers are handled anonymously, multiple judges or prosecutors handle a case together, and 8% occasionally refuse a case for safety reasons.

The fear of escalation also affects private life and decision-making. Prosecutors and judges shield information, take extra security measures, and sometimes consider quitting. Moreover, several prosecutors and judges have indicated that they would never want to work on a case like the Marengo trial or handle a case for which they require security. Additionally, a large proportion of the respondents, around ninety percent, are concerned about the hardening of the underworld and its influence on the rule of law.[187] The research shows that organised crime not only causes direct physical risks, but also undermines the resilience of the rule of law through (visible) intimidation, threats, and physical violence against legal professionals.

Box 6.6

Example of pressure on journalists
In a 2025 interview with crime journalists Belleman and Van Den Heuvel in *HP de Tijd*, Van Den Heuvel states that he has been provided with security since he began writing about T.'s group. Belleman and Van Den Heuvel refer to attacks on the editorial office of *De Telegraaf* and on the premises of *Panorama*, in which a rocket launcher was used. They also indicate that intercepted PGP messages revealed that there were concrete plans to carry out an attack on the *RTL Boulevard* studio. According to the interviewees, the murder of Peter R. de Vries has left a deep impression. It has caused fear within journalism, with Belleman stating that you do become more cautious about everything you write. Moreover, colleagues have stopped and sources have become more reserved. In their view, fear has crept in not only within journalism, but also among judges, lawyers, the Netherlands Police, and the OM as a result of the violence stemming from organised crime.[188]

Box 6.7

Example of leaking information to criminals
On 18 March 2025, the Overijssel District Court (The Netherlands) sentenced a 40-year-old former police officer to eighteen months' imprisonment for multiple counts of unlawful access to a computer system, breach of official secrecy, and leaking confidential information from police systems in exchange for money. Between 2016 and 2020, he gained unauthorized access to police data regarding individuals and ongoing investigations and provided this to a 37-year-old co-defendant from Almere, who paid him for this. In total, this involved approximately fifteen queries. The court ruled that the former officer had seriously damaged trust in the Netherlands Police and had abused his position.[189]

Box 6.8

Furthermore, political-administrative harm arises when criminal networks have influence or a position of power in political-administrative infrastructures. Consider the possibility that accomplices are members of the municipal council and thus have access to the municipal government and/or can influence decision-making within the municipal council. Influence or a position of power in social or economic infrastructures also leads to harm. The Dutch government's control over its own territory is compromised if criminal networks are able to exert significant influence or hold a position of power in certain economic sectors or at specific locations (see also section 6.4). As a result, the government may lose control over what takes place within them.

Political-administrative harm also arises when officials of the rule of law become involved in organised crime. Although a complete overview is lacking, examples of involvement are known within various government sectors. Government officials are attractive targets because they have access to systems and information and hold formal powers (see section 3.2.4). Abuse of government systems, services, and products will put public trust in government processes under pressure. For example, the government holds sensitive personal information of citizens, which citizens are required to provide. Abuse of this information undermines trust in political-administrative infrastructures, as well as their vitality. The leaking of investigation information, for instance, undermines the effectiveness of investigation and can contribute to the other sources of harm mentioned in this paragraph.

Finally, political-administrative harm arises when criminal networks meet societal needs. This contributes to the influence and power position of criminal networks in sectors or neighbourhoods and causes political-administrative harm as the government may lose control over those sectors and locations. See sections 6.4 and 7.2 for further details.

6.4 Social harm caused by subversive activities

Subversive activities lead to social harm. They affect social cohesion and objective and subjective safety, particularly within local environments or specific population groups. According to the SCP, social cohesion concerns the extent to which (groups of) people feel connected to one another and to institutions, and demonstrate this in their behaviour. It is about 'the glue' that holds communities together.[190]

In terms of social cohesion, a distinction can be made between horizontal and vertical connections. Horizontal connections relate to the trust and connectedness that (groups of) citizens experience among themselves, for example between neighbours or within social networks. Vertical connections relate to citizens' trust in the government[191], specifically focusing on the government's ability to provide for basic needs pertaining to the social domain: the facilities, resources, and social services that citizens require to meet their basic needs and maintain their quality of life.*

In the STAN, the assumption is that social harm is primarily caused by:

1. Manipulation through influence over or a position of power in neighbourhoods or companies.
2. Recruitment and deployment of citizens and companies in subversive activities.
3. Integration of illegal proceeds into society.
4. Criminal networks meeting societal needs.

A major cause of social harm is the degree of influence that criminal networks have on neighbourhoods, associations, or population groups, often in combination with a level of power in that environment. For their business operations, they require access to locations, including logistical hubs, storage facilities, and meeting places, and they often rely on their own social environment for 'personnel' (see section 2.1). To shield operations and finances, a safe environment is essential in which few questions are asked and no reports are made to the authorities.

* In a narrow sense, social needs refer to the provisions that ensure individuals in society have a basic level of well-being and security, such as welfare benefits, healthcare, housing, and education. In a broader sense, the term also refers to individuals' need to feel connected and valued. The SCP adopts this broader definition.

Examples of the grip of organised crime on neighbourhoods

In 2023, the mayors of Amsterdam and Rotterdam described in a letter a bleak picture of the growing grip of organised crime on their cities. The most vulnerable local communities are at risk of being poisoned by criminal money. They cite two examples where close-knit criminal networks have a firm grip on young people. Major drug criminals employ extreme violence throughout the entire drugs trafficking chain in the Netherlands. The mayors express concern about ending up in a criminal and violent culture that is gradually taking on characteristics reminiscent of Italy. This concerns not only conflicts over the control of the drugs market, but also violence as a display of power aimed at undermining the democratic rule of law.[193]

In September 2025, the Brabants Dagblad reported that in Eindhoven (a city in the Netherlands), criminal networks have exerted de facto control over the street scene and certain locations around Kruisstraat and Woenselse Markt (a street and square in Eindhoven) for an extended period. Crime, nuisance, and public order disturbances have been present there for some time. Repeated drug investigations showed that hospitality establishments, commercial properties, and residences around Kruisstraat were involved in drug trafficking, money laundering, and other subversive activities.[194]

Box 6.9

Example of social position of power in sport clubs

There are indications that criminal interference occurs at amateur sports clubs across the country,[195] ranging from rumours about criminal sponsors[196] to facilities being used by criminal networks as a meeting place.[197] Furthermore, criminal networks can use this environment to bring young members into their sphere of influence, specifically targeting vulnerable youth.[198] In local neighbourhoods as well, criminal networks can build a social position of power by flaunting their status or actively recruiting youth. They can offer young people struggling with inequality of opportunity and social exclusion an alternative path to status and recognition.[199]

The acceptance of money of suspicious origin by amateur sports clubs can lead to a donor claiming influence or acquiring social status within a sports club. Criminal influence can also affect the club culture: it creates opportunities for drug deals on the premises, people with a criminal background appear around matches, and board members or employees may be pressured or even threatened when they wish to take a different course.[200]

Box 6.10

Examples of socio-moral harm mentioned by Teun Voeten

"Crime creates an alternative pattern of values and norms in which the essential building blocks of social cohesion, such as responsibility, care, and solidarity, are dismantled. Conversely, selfish pursuit of profit, greed, materialism, opportunism, and short-term thinking become central. [....] On a moral level, the criminal lifestyle becomes a desirable way of life. [....] Many people in the immediate surroundings benefit, but in every criminal culture a kind of omerta prevails, where people remain silent towards the outside world out of fear or group solidarity. One consequence is that a dwindling trust in the government arises among law-abiding citizens, while cynicism and indifference increase. This is a very harmful development that profoundly undermines social cohesion, the backbone of every democratic, open, and solidary society. [....] This is reinforced by the ostentatious behaviour of criminals. [....] This causes frustration not only among citizens, but also among so-called frontline workers."[201]

Box 6.11

An increasing role of criminal networks in neighbourhoods undermines horizontal social cohesion. Citizens and businesses that participate have an advantage over those who do not. Crime can be seen as a life path that offers respect, income, and status. The normalisation of criminal behaviour is also a risk: activities that once seemed unacceptable may become accepted over time.

Communities with little trust in the government, but high trust in fellow citizens, can develop into safe havens where the government is seen as an adversary rather than a partner. As a result, the government loses its grip on these neighbourhoods.

The presence of criminal networks also has an intimidating effect, particularly when they are influential and thereby undermine objective and subjective safety. If this presence and influence continue to strengthen, citizens may no longer feel free to move, express themselves, or intervene when they notice irregularities. The presence of production sites in neighbourhoods and the storage of illegal commodities or money entails risks. This includes the dangers of drug labs in neighbourhoods, as well as rip-deals or acts of retaliation involving violence. Especially incidents that receive media attention or experiences in one's immediate environment can lead to feelings of fear, frustration, and anger. Furthermore, the idea that criminals exert influence over the local environment, and that they are able to operate freely, intimidate people, or dictate rules, can cause an increased sense of vulnerability among residents and society at large.

Criminal networks may continue to strengthen their influence in society by (continuing to) meet needs that the government or organisations do not meet, do not meet to a sufficient extent, or only meet at higher prices or under strict conditions. According to Tops and Van der Torre, large sums of money circulate within the (supralocal) criminal economy in vulnerable areas. "Depending on the exact neighbourhood or area characteristics, this involves tens or hundreds of millions on an annual basis, and possibly significantly more." They state that criminal money acts as a lubricant at the neighbourhood or village level.[192] By providing opportunities to obtain a mortgage, subletting properties they own (see box 6.12), providing an alternative source of income, or investing in a (local) social organisation (see box 6.10), they create an alternative system in which citizens become dependent on the criminal structure. Criminal networks can also take over roles by offering citizens a listening ear and recognition, causing individuals to rely on criminal networks.

Example of meeting needs

The Amsterdam police reported in 2025 that they had encountered criminal networks that, in exchange for payments usually amounting to several thousand euros, commit mortgage fraud. The mortgage fraudsters facilitate houses for citizens who want to artificially inflate their reported income. They also provide housing for drug criminals, pimps, and labour exploiters, with the properties being used for storing drugs, as safe houses for criminals, and to house (illegal) migrant workers. It is estimated that around 60 million euros in criminal assets were earned through this. Detectives and officers from various police units all indicate that they have encountered criminal networks that commit mortgage fraud. "We believe that fraud was committed during the purchase of approximately 8,000 homes in recent years," says an Amsterdam police chief.[202]

Box 6.12

6.5 Ecological harm caused by subversive activities

Some subversive activities cause harm in people's immediate living environment and to the natural environment. This harm is not limited to immediately visible harm, such as the dumping of chemical waste. It can also involve harm that gradually affects the quality of life, the living environment, the soil, the water, and biodiversity.

The immediate living environment is affected by harmful substances released during drug production, waste dumping, residual waste, and environmental damage resulting from violent incidents. These activities lead to a structural disruption and pollution of the public space. This directly affects the safety and liveability of neighbourhoods. In addition, natural areas such as forests, heathlands, and agricultural lands are affected by the dumping of chemical waste. This leads to soil damage, causing long-term harm to flora and fauna. Harmful substances can seep into surface water and groundwater, which has consequences for aquatic organisms, plants, and animals. When agricultural land and natural drinking water become contaminated, harmful substances can enter food chains. This poses a risk to public health and ecosystems.

Additionally, exposure to toxic substances that are released during the production of drugs, for example, can cause harm to health. Most of these harmful effects, such as complaints involving the respiratory tract, eyes, or skin, are mild. These include, for instance, headaches, dizziness, skin irritation, respiratory irritation, a persistent cough, or nausea. Repeated or prolonged exposure can have serious consequences. For example, direct exposure to alkaline in the eyes during an explosion or the inhalation of phosphine can cause serious damage to the eyes and respiratory tract.[203]

Illegal trade in plants and wildlife creates conditions in which diseases spread easily. For example, the illegal trade in wildlife can lead to zoonoses. These are diseases that jump from animals to humans, such as SARS, COVID-19, HIV, Q fever, and Ebola. During transport, animals are kept in close proximity under poor conditions, where they come into contact with each other's blood and excrement. Furthermore, stress and malnutrition lead to reduced immunity. These conditions are therefore a breeding ground for diseases. When these diseases jump to humans, the consequences for human health can be severe, such as mortality and epidemics.[204]

Harmful effects of drug production

In 2024, 167 drug labs were dismantled, a record number according to the Nationaal Overzicht Drugslocaties 2024 (National Overview of Drug Locations). More than half were located in residential areas. The Netherlands Police found them in regular homes and apartments, but also in sheds, garages and commercial buildings. The dumping of drug waste also increased: 217 reports. These often involve jerrycans or drums left behind in natural areas, on deserted roads, or in public underground waste containers. Drug criminals also dump waste directly into the soil, which entails additional risks for the environment and public health.[206]

In Baarle-Nassau (the Netherlands) in 2024, manure mixed with waste from crystal meth production was spread on three fields, the police reported. The owners of the plots on which onions were being cultivated have been questioned as suspects, Omroep Brabant reported. According to the police, criminals are increasingly dumping drug production waste directly into the soil, making contamination less visible and leading to prolonged legal disputes over who is responsible for cleanup costs. Experts warn that the scale of this problem remains largely unknown.[207]

Box 6.13

In the "Dreigingsbeeld Milieucriminaliteit (Environmental Crime Threat Assessment) 2021", attention is given to various forms of environmental crime linked to organised crime. These offences cause various types of harm, including ecological harm. Some of these are immediately noticeable, such as soil pollution, while other harm, such as greenhouse gas emissions or the degradation of biodiversity, becomes apparent primarily in the long term.[205]

6.6 Harm to the international reputation of the Netherlands due to subversive activities

The Netherlands is perceived as a country that plays a significant international role in organised (drugs) crime and may be seen as a country that is insufficiently capable of protecting itself against it (see box 6.14 for some indicators). This may have consequences for foreign investment appetite in the Netherlands, cooperation in the field of security and law enforcement, diplomatic relations, and the overall position of the Netherlands within international bodies. This process does not occur abruptly, but manifests itself gradually as the consequences become visible to other states and international partners.

The role of the Netherlands in organised crime leads not only to illicit proceeds in the Netherlands, but also abroad. For instance, Dutch criminal networks not only export the synthetic drugs produced in the Netherlands, but also the associated problems. Organised crime is transnational and criminal networks in the Netherlands are connected to criminal networks abroad.[208] At the same time, smaller criminal networks primarily operate regionally and locally, while larger ones more often operate internationally.[209] For Dutch organised drug crime, for example, criminal networks mainly operate in and from the Netherlands, but are also active abroad to facilitate trade.[210] In this way, they also contribute to the influence and/or position of power that criminal networks abroad acquire through the trade and profits they achieve with these Dutch products (see box 6.15).

No recent and reliable data have been found regarding the international role of the Netherlands in global money laundering by organised crime. Reports from the FIOD refer to an estimate of €13 billion per year for money laundering in its entirety, although the reference date is not clear.[211] The National Risk Assessment Money Laundering (National Risk Assessment Witwassen) 2023[212] is based on a 2018 study by the WODC, but the underlying figures are based on data up to and including 2014. FIU the Netherlands states in the 'Annual review FIU the Netherlands (Jaaroverzicht FIU-Nederland) 2024' that over €17 billion in suspicious transactions were reported by reporting entities[213] , but these reports do not apply exclusively to organised crime.

International perspective on the Netherlands in relation to organised crime

Various internationally authoritative reports present a consistent picture of the role of the Netherlands within international organised crime, in particular the drug economy. Europol stated in 2024 that Belgium, the Netherlands, and Spain report the highest volumes of cocaine seizures, which underscores their significance as European gateways.[214] Europol stated in 2021 that Dutch actors are overrepresented in large-scale cocaine smuggling and that the ports, especially Rotterdam, fulfil a central logistical function in the distribution to the European hinterland.[215] In 2023, the UN described the Netherlands as "a major cocaine hub in Europe".[216] And the US Department of State stated in 2025 that "the Netherlands plays a key role in the international drug trade".[217]

This perception leads to political attention and criticism from abroad. While the Netherlands is generally seen as an indispensable partner that must take responsibility, direct accusations are also being made. For instance, in 2024, the then French Minister of Economic Affairs warned the Senate that, regarding the production of synthetic drugs, the Netherlands is well on its way to becoming what Colombia is for cocaine, risking the emergence of "new Medellíns in the heart of the European continent".[218] A similar sentiment was expressed in Belgium: in 2018, the then mayor Bart De Wever stated that "drug-related violence is spilling over from the Netherlands,"[219] and in 2024, he called the Netherlands "the narco-state of Europe".[220]

Box 6.14

Financial estimates CBS 2021 of the production of and trade in cocaine, synthetic drugs and cannabis

CBS estimated for 2021 that €15.5 billion was earned within the national borders from the production of and trade in cocaine, synthetic drugs and cannabis, of which €3.6 billion could be attributed to the Dutch economy. The remainder was attributed to clients abroad in accordance with European guidelines. Particularly in the trade in cocaine, there is a large difference between what is earned within the national borders (€10.7 billion) and what forms part of the Dutch gross domestic product (€1.2 billion). It is estimated that 98% of the synthetic drugs produced in the Netherlands are destined for export. In 2021, 3.2 billion was earned from the production of synthetic drugs in the Netherlands, of which 1 billion remained in the Dutch economy.[221] This makes it clear that the production of and trade in cocaine, synthetic drugs and cannabis from and/or via the Netherlands not only leads to criminal proceeds in the Netherlands, but also in other countries.

Box 6.15

6.7 Subversive effects strengthen system vulnerabilities

When subversive effects occur, they can lead to new system vulnerabilities or reinforce existing ones. This can create a self-reinforcing mechanism in which harm to society is not only the result of subversive activities but also contributes to them.[222] For example, the presence of criminal networks in neighbourhoods has an intimidating effect. As a result, citizens' trust in the government and in each other can be undermined. This can create a climate in which criminal networks thrive, as it may be accompanied by a decrease in the willingness to comply with rules or report abuses, a decrease in the (normative) authority of the government[223] , and a decrease in informal social control. This is a highly simplified example. In practice, it concerns a dynamic - rather than 'linear' - interaction between diverse subversive activities, effects, and system vulnerabilities.

Example of dynamic interaction

The investment of illicitly obtained funds in residential property by criminals, for the purpose of money laundering, can drive up housing prices in neighbourhoods and displace legitimate buyers. This affects the liveability of these neighbourhoods, as criminals gain influence and use properties to store illegal commodities such as weapons, drugs, or money, and/or to accommodate other criminals, resulting in unsafe situations. This can lead to additional vulnerabilities in these neighbourhoods and contribute to the normalisation of crime in those areas. As housing is withdrawn from the regular market, this can further exacerbate housing shortages, from which criminals may further profit. Greater dependency on and/or influence of criminals, combined with (the threat of) violence by criminals, can result in a culture of fear in which people are reluctant to report matters to the authorities. This, for example, makes the oversight of real estate transactions even more difficult.[224]

Box 6.16

7

Threats

Photo: According to the General Intelligence and Security Service (AIVD), criminals regularly attempt to ensure that criminal rivals attract media attention in the hope that they will come to the notice of the police and judicial authorities. "Such manipulation is dangerous for journalists, because members of criminal networks may regard them as an extension of rival groups or law enforcement agencies." (Translated by author) (See Box 7.10)

Subversive crime by organised crime undermines the rule of law in an insidious and often invisible manner and poses a threat to national security. There is a risk that the role of organised crime in society is increasing, while society's grip on organised crime is decreasing due to its own vulnerabilities. Identified threats paint a bleak picture of the future.

These threats are:
1. *Social safety net by organised crime.*
2. *Oil-spill effect of involvement in organised crime within society.*
3. *Influencing decision-making and the functioning of institutions through structural manipulation by criminal networks.*
4. *Illegal proceeds find their way into society through the diverse use of financial channels.*
5. *Cumulative harm due to the intertwining of criminal networks with state or ideological actors.*

These threats, when manifested, lead to the impairment of national security, specifically the national security interests of economic security and social and political stability.

7.1 Threats do not provide a snapshot of the current situation

Five threats are described in this chapter. These threats primarily outline what we may expect. Four of them were established based on the combinations of subversive activities described in Chapter 6, which, individually and in combination, cause economic, political-administrative, and social harm. While the emphasis in the previous chapter was on the perspective of criminal networks, the perspective of society was chosen for the threats. For example, instead of 'recruitment and deployment by criminal networks', this has been mirrored in the threats as 'involvement of society'. A fifth threat has been added separately, namely the threat concerning the intertwining of criminal actors with state or ideological actors. This is based on geopolitical developments and the analysis of documents. The threats have been analysed in combination with the goals of criminal networks, system vulnerabilities and/or broader developments as described in previous chapters. This combination determines the extent of the threat.

Sometimes examples of (parts of) the threat are already known, but this analysis often involves the interpretation of weak signals or plausible reasoning without hard facts. If only what is already happening were to be described, intervention may be too late. This is entirely due to the dormant nature of subversive crime (see section 6.1). The threats therefore do not constitute a 'snapshot' of the current situation.

Just as spotlights are focused on specific parts of the stage during a play, this chapter focuses on individual threats within the broader threat landscape of subversive crime. Although threats exist independently, they also influence and reinforce one another. For instance, threat 1 (social safety net by organised crime) can contribute to threat 2 (the oil-spill effect of involvement in organised crime within society). Other threats from the security domain also come into play. This applies, for example, to digital threats such as cyberattacks by cybercriminals and the threat posed by state actors. This interconnectedness provides points of leverage to develop an approach that does not focus specifically on the mitigation of a single threat, but on multiple threats, and in combination with other security domains. If resilience increases broadly, this also has an effect on resilience against subversive crime.

For each threat, the subversive effects are also addressed when the threat manifests. This includes a brief look at the types of harm as described in Chapter 6. Additionally, these are translated into so-called national security interests (see box 7.1). Since national security interests are used for a wide variety of security issues and were originally primarily focused on so-called 'flash incidents' (for example, a breach of a sea dike) rather than slow-onset threats, the security interests and the underlying so-called impact criteria are not easily applicable to a domain such as subversive crime.[225]

The order of the presented threats is not intended as a ranking. Such a ranking is difficult to make objective. After all, many variables influence the extent of a threat and the subversive effects when the threat materialises. Furthermore, the threats influence or reinforce each other, as indicated above.

National security interests[226]

Territorial security:
The uninterrupted functioning of the Netherlands and its EU and NATO allies as independent states in a broad sense, or territorial security in a narrow sense.

Physical safety:
The uninterrupted functioning of people in the Netherlands and their environment.

Ecological security:
The uninterrupted continued existence of the natural living environment in and near the Netherlands.

International legal order:
The proper functioning of the international system of norms and agreements, aimed at promoting international peace and security.

Economic security:
The uninterrupted functioning of the Netherlands as an effective and efficient economy.

Social and political stability:
The uninterrupted continuation of a societal climate in which individuals can function without disturbance and groups can peacefully coexist within the institutions and principles of the Dutch democratic rule of law and its shared values.

Figure 7.1

7.2 Threat: Social safety net by organised crime

There are indications that criminal networks offer alternatives to 'social services' that are not, or are insufficiently, accessible or available to (vulnerable) citizens and companies, or are only available under specific conditions, such as a doctor's prescription, or at higher prices. Examples include the need for housing or physical protection, care, medicines that someone cannot obtain by prescription, or loans. When citizens or companies accept this offer, they become increasingly dependent on criminal networks. The self-interest of criminals dominates, and classic 'quid pro quo' relationships emerge. In this way, criminal networks may request favours from vulnerable persons in exchange for housing or debt restructuring. Examples include helping with cannabis cultivation or illegal prostitution.

Underlying interest for organised crime

Criminal networks may have a strategic interest in creating a social safety net for citizens and businesses. This not only generates money, but also allows them to better shield their activities and strengthen their power. It should be noted that this interest is partly dependent on other sources of income in combination with the associated risks.

Infrastructures and vulnerabilities exploited by criminal networks

A characteristic of organised crime is that it capitalises on (among other things) needs (see section 2.2). The Advisory Committee on Strengthening the Resilience of the Democratic Rule of Law in the Netherlands (Adviescommissie Versterken Weerbaarheid Democratische Rechtsorde) stated the following at the end of 2023: "There are residents who are systematically disadvantaged by the way the democratic rule of law currently functions. Disadvantaged to such an extent that the social fundamental rights mentioned in the Constitution (such as the right to housing, livelihood security, social security, healthcare and education) are not being realised."[227] Economic sectors through which criminal networks can offer a social safety net include, for example, the housing market, labour market, educational institutions, training institutes, healthcare institutions and daycare centres.

Examples of 'social services'

In 2023, the Netherlands Police in Limburg warned entrepreneurs who were in financial distress due to the 2021 floods around Valkenburg (a municipality of Valkenburg aan de Geul, the Netherlands) not to get involved with criminals. According to the mayor of Valkenburg aan de Geul, government assistance for affected entrepreneurs did not get off to a good start. Instead, hospitality entrepreneurs were offered financial assistance from the criminal underworld. Criminals approached vulnerable entrepreneurs to launder their money, facilitate drugs trafficking, or make meeting rooms available.[230]

According to research by the Trimbos Institute, an estimated half a million Dutch people use cannabis to alleviate physical and psychological complaints. Only a fraction of these - approximately 7,000 patients - are prescribed cannabis through regular healthcare. The remaining users turn to coffeeshops or home cultivation, despite the associated risks, such as potential contamination and uncertainty regarding the THC and CBD content. Many users would prefer to receive medicinal cannabis by prescription due to the controlled quality and composition. However, they encounter obstacles such as insufficient knowledge among doctors and patients, fear of stigmatisation, a limited product range, and high costs. Since 2018, medicinal cannabis has no longer been reimbursed by health insurance, making it unaffordable for many chronically ill people.[231]

Box 7.2

Certain system vulnerabilities make groups, neighbourhoods, and sectors vulnerable. Neighbourhoods are vulnerable when a certain degree of normalisation of crime is present and/or when trust between citizens and in the government has declined. Examples of vulnerability for citizens include financial hardship, illegal residence in the Netherlands, falling through the cracks regarding healthcare services, chronic pain complaints, problems with childcare, or an insufficient level of education to keep up in the labour market. For sectors and companies, consider financial hardship and government measures that, for example, put pressure on profitability or are aimed at contraction, such as in the agricultural sector and fisheries. Negative perceptions of the government and politics also play a role. Situational factors can also create vulnerability. Examples of situational factors include economic crises, rounds of layoffs, epidemics, or natural disasters.

There are more system vulnerabilities that contribute to criminals providing a social safety net, such as "unintentional government facilitation," "limitations in laws and regulations," and "limitations in the approach" (see section 3.3). This concerns, for example, late detection, an incomplete picture, or possibly even a missing legal framework for intervention. For instance, the Netherlands Police, mortgage lenders, and notaries are calling on legislators to introduce policy measures to prevent properties from falling into the hands of criminals through mortgage fraud. "The current legislation provides far too much leeway for the criminal. What we would very much like, for example, is for mortgage lenders, including banks, to be able to verify income levels with the Dutch Tax Administration. Because that is not possible now," said an Amsterdam police chief.[228] During an expert meeting, it was noted that in a particular street in a city, criminals were buying up houses that had been put up for sale by investors due to government measures in the housing market. This type of information can hardly be shared with the relevant parties.[229]

Assessment

Criminal networks have a strategic interest in providing a social safety net. Although not on a large scale, there are already indications in the Netherlands that criminal networks are engaging in this. Examples of this are certainly known in South American countries. Structural and situational factors create a need among (groups of) citizens and companies. Political choices and government policy also influence the extent to which citizens and/or companies are vulnerable to assistance from criminal networks. In any case, opportunities exist for criminal networks.

Providing a social safety net leads to the undermining of national security, in particular social and political stability, economic security and potentially also territorial security. Gradually, criminal networks may increasingly provide a social safety net making parts of society dependent on this provision and thereby expanding their influence and power in society. This influence and power have a negative impact on social cohesion and/or objective and subjective safety in neighbourhoods. A broader base for the recruitment of others into criminal activities may also emerge. For instance, criminal networks may request favours from vulnerable persons in exchange for housing or debt restructuring. Examples include assisting in cannabis cultivation or illegal prostitution. This influence and power also undermine trust in political-administrative infrastructure, and the government potentially loses control over its own territory. Furthermore, it affects economic security when, for example, criminal services disrupt markets, such as when criminal networks withdraw housing from the regular market. This offer can also be accompanied by fraud, for example mortgage or healthcare fraud, also resulting in economic harm.

7.3 Threat: Oil-spill effect of involvement in organised crime within society

Involvement in organised crime can spread through society like an oil spill. Organised crime then becomes further embedded, making the distinction between the upper and underworld increasingly difficult to draw. Criminal networks are, in any case, dependent on and part of both legal and illegal ecosystems. For many years, they have been involving young people, other citizens, officials within specific professional groups and (employees of) organisations in their illegal activities. This involvement varies in degree, and the initiative can originate from both criminal networks and the individuals involved.

Underlying interest for organised crime

Just like legal enterprises, criminal networks cannot function without the involvement of others to obtain the necessary capacity, knowledge, services, and products (hereinafter capacity). This capacity is required for business operations, shielding, the strengthening of power, and access to locations, resources, documents, and information. Although recruiting personnel from their own social network offers significant advantages, they often cannot avoid recruiting outside it as well. Not all required capacities are available within their own network, and they must sometimes make use of legal infrastructures.

Infrastructures and vulnerabilities exploited by criminal networks

Involvement varies in degree, and the initiative may originate from either criminal networks or vice versa. Economic, political-administrative, and social infrastructures are all susceptible to involvement. For example, the deployment of young people provides strategic added value for criminal networks (see section 4.1).

Criminal networks also recruit citizens with relevant knowledge, experience, or skills who are employed in specific economic, political-administrative, or social sectors. Citizens with access to sensitive data, logistical or technical knowledge, and financial expertise are valuable or sometimes even essential. For instance, according to the WODC, corruption was evident in all examined criminal investigations into groups involved in the importation of cocaine to or via the Netherlands. This appears to be related to the tightened security measures. Consequently, internal cooperation is essential for the successful importation of cocaine.[232]

Vulnerabilities that motivate individuals to become involved with criminals range from financial problems and a negative perception of norms to a lack of trust in the government. Developments such as individualisation increase the vulnerability of citizens by placing self-interest above the public interest and making individual considerations decisive, such as the pursuit of luxury and quick money. Through digital platforms such as Snapchat and games, citizens can easily respond (directly) to jobs.[233] Involvement also arises through 'criminal intermediaries', facilitators who recruit personnel for carrying out jobs (see section 2.2.4). These often concern so-called 'high-risk activities' such as providing cover functions for production, transport, extraction, and carrying out contract killings. This allows core members of criminal networks to limit their risks. Conversely, citizens can offer their own skills via digital platforms, among other channels. This creates a market in which supply and demand meet with increasingly lower barriers.

Cash Compensation Model as example of involvement

A particular form of involvement is one in which criminals meet the need for illicit cash by companies by means of the so-called Cash Compensation Model (CCM). CCM is a scheme in which professional money launderers 'sell' criminal cash to companies. These companies pay for this via bank accounts of legal entities with front men, often on the basis of false invoices. An analysis (2024) by FIU the Netherlands and banks within the Fintell Alliance revealed a network that presumably operates according to this model. Via dozens of legal entities, the managed bank accounts received payments from more than 150 companies, primarily from labour-intensive sectors such as transport, healthcare, and construction. The cash can then be used to pay staff entirely or partially off the books, which provides a tax advantage. The money received via the bank accounts is spent, among other things, on luxury vehicles, gold, and purchases abroad that seem to be unrelated to the business activities. This may indicate additional forms of money laundering, tax fraud, and third-party payments.[234]

Box 7.3

Three lawyers suspected of passing messages to the outside world

Three lawyers of Ridouan T. were arrested in 2021, 2023, and 2025 respectively, on suspicion of passing on messages to people in his network outside prison. One lawyer was sentenced to 5.5 years in prison in 2023.[238] The legal proceedings against the two other suspects were still ongoing in February 2026.

Because a perception has emerged that criminal defence lawyers are willing to exchange information with the outside world on behalf of their clients, criminals sometimes wrongly assume that lawyers are willing to do so. This can lead to threats if a lawyer does not cooperate.[239]

Box 7.4

The line between citizens who, on their own initiative, provide knowledge, services, or labour to criminal networks and citizens who are unknowingly exploited or influenced can be razor-thin. Whether citizens are unaware or consciously look the other way provides essential insight into the structural vulnerability of society with regard to organised crime.[235]

There are several reasons why companies are useful for criminal networks, including money laundering, tax fraud, and facilitating and concealing activities.[236] Criminal networks set up companies themselves, or use existing companies with or without the knowledge of the directors or owners. Although companies in financial distress are more susceptible to takeover by criminals or to partnering with criminals, there are examples of criminals specifically targeting companies with a good reputation. After all, it is less likely that these companies will be suspected of involvement.

Criminal networks sometimes cannot operate without the facilitating services of liberal professions. Due to the expertise of these professional groups and the nature of their activities - where they, among other things, provide legitimacy to legal entities or commodities by means of documents - they are an attractive group. These services are, for example, necessary for money laundering or real estate transactions. Examples of attractive liberal professions that can (unconsciously) facilitate criminal activity include lawyers, notaries, accountants, and tax advisors.[237] See also section 3.2.3

Illustration (possible) Involvement of companies

Legal companies and legal entities are increasingly becoming a crucial link in the modus operandi of criminal networks. In 2024, FIU the Netherlands received nearly 3.5 million reports of unusual transactions, a significant increase compared to 2023, in which companies played a facilitating role in a substantial part of the files. In particular, private limited companies are used to conceal ownership structures, mask financial flows, or purchase raw materials for drug production.[240] According to Europol, 86% of the most threatening criminal networks use legal business structures to organise, shield, and legitimise their activities.[241]

The management of a company operating in a port had been involved in cocaine trafficking for 6.5 years, according to the public prosecutor during the first procedural hearing in 2024. According to the Public Prosecution Service (OM), the three directors are suspected, among other things, of importing cocaine from South America, forgery, and participation in a criminal organisation. The (suspected) mixing of legitimate business operations with illegal activities led to administrative closure and ultimately bankruptcy. This had direct consequences for employees, creditors, and the regional port function. The directors deny the allegations. The substantive hearing of the criminal case is expected to start in June 2026, with a judgment expected in September 2026.[242]

Shipyards are used for the production of amphetamine, where access to water and storage facilities offers logistical advantages. Holiday parks offer anonymity and seclusion and are used for production, transport, or waste dumping. Ports and logistics companies form the infrastructure for the transport, transshipment, and distribution of drugs, weapons, and people, where commodities are often disguised.[243]

Box 7.5

Assessment

Criminal networks have a strong interest in involving citizens and organisations within and outside their own social network. There are sufficient examples of the involvement of young people, (employees of) organisations, civil servants, and a few cases of well-known Dutch nationals. Involving others outside their own social network does entail risks due to the illegality, but loyalty is enforced by (threatening to) apply psychological or physical violence. Various vulnerabilities and developments can - either individually or in combination - lead to involvement, namely: the financial attraction of organised crime combined with the desire for status and making money quickly, the opportunities offered by digital platforms for establishing contacts, and financial, psychological and/or mental vulnerabilities. Limitations in the approach to combat organised crime and in laws and regulations may contribute to a ripple effect because involvement is not detected in time or because the pull effect of digital platforms cannot be reversed.

Involvement that spreads through society like an oil spill undermines the security interests of economic security and social and political stability. It leads to economic, social, as well as political-administrative harm. Through large-scale involvement, criminal networks can continue their business operations and thus build up even more illegal assets, shield assets and activities, and minimize risks, while strengthening their influence and position of power. At the same time, economic, political-administrative, and social infrastructures become entangled with criminal networks. Moreover, this can contribute to the normalisation of criminal behaviour. When they no longer wish to cooperate, criminal networks can put pressure on those involved using (the threat of) violence. This creates a downward spiral.

7.4 Threat: Influencing decision-making and the functioning of institutions through structural manipulation by criminal networks

When criminal networks have built up significant interests in illicit markets or in society, and those interests come under pressure, criminal networks will seek to strategically and structurally manipulate societal decision-making and the functioning of institutions. If they succeed in this, criminal interests will be taken into account, consciously or unconsciously, in decision-making and the exercise of public functions, for example, to avoid violence or other problems.

Manipulation is understood broadly in this context and encompasses a wide range of forms and degrees. It can manifest in attempts to deliberately influence or steer legislation and regulations, administrative decision-making, law enforcement, and the exercise of government functions. This can be achieved through the strategic and systematic corruption of officials, or by infiltrating institutions of the democratic rule of law. In this way, criminal networks, for example, gain access to crucial decision-making processes, information systems, and key figures with relevant powers or access rights. Manipulation also includes engaging in a conflict with 'adversaries' by putting them under pressure, threatening them, assassinating them in a high-profile manner, or spreading disinformation. Adversaries may be criminal rivals. Officials of the rule of law are also considered adversaries, such as police officers, judges, public prosecutors, regulators, administrators, politicians, journalists or lawyers and/or others from society, including gatekeepers and (employees of) companies or citizens.

Possible threat of organised crime towards authority figures according to media reporting

In September 2022, media reported that Crown Princess Amalia and the then-Prime Minister Rutte were given additional security because they were considered potential targets of an attack or kidnapping by criminals. This was said to have emerged from intercepted communications. The kidnapping was said to potentially serve the purpose of securing the release of a criminal kingpin. Although the authorities did not comment on the threats and security measures, the then-Minister of Justice and Security described the threat of organised crime in general as "very substantial". She stated that guardians of the rule of law, such as journalists and mayors, were under increasing pressure because they "want to continue doing their work and criminals do not agree with that."[246]

Media reported in September 2022 that a kidnapping of the Belgian Minister of Justice had been thwarted by a joint operation of Belgian and Dutch investigative services. This was prompted by indications that four suspects intended to kidnap the minister in his place of residence. According to statements by the Belgian authorities and the minister himself, the attempted kidnapping was linked to the drug trade. The suspected background of the threat lay in the intensification of Belgian policies against drug crime. Additionally, the minister's central role in cracking encrypted criminal communication networks and facilitating international cooperation on the extradition and confiscation of assets from drug criminals was said to have played a role.[247]

Box 7.6

Underlying interest for organised crime

Some criminal networks have built up significant interests in illicit markets, economic sectors and/or neighbourhoods. Maintaining that power is a goal for criminal networks. In any case, they have an interest in remaining under the government's radar. If the government were not to hinder them in the slightest, there would be no immediate need to manipulate government processes to maintain power. When criminal networks feel their existence is threatened, it is plausible that they will actively engage in conflict with their 'opponents'. Employed counterstrategies are often a direct reaction to an increased power struggle or disputes between criminal networks, and/or successful government action and/or growing social resistance. For example, foreign criminal networks establishing themselves in the Netherlands can shake up existing power positions. Criminal networks could increasingly resort to rip deals, tip off law enforcement agencies about shipments, or start stealing cash, while the authorities continue to pursue criminals.

Infrastructures and vulnerabilities exploited by criminal networks

Criminal networks have a strategic interest in manipulating the legislative power, as it potentially offers them benefits and can limit risks.[244] Manipulation of the legislative power can take place at various levels: municipal councils, provincial councils, the House of Representatives (De Tweede Kamer), the Senate (De Eerste Kamer), the European Parliament, as well as in other governing bodies such as water boards (regional water authorities). Structural manipulation at the municipal level can, for example, lead to criminal networks gaining influence over local regulations, such as spatial planning regulations that support construction and hospitality interests. At national and international levels, such manipulation can result in laws and regulations that may prove advantageous for criminal networks.[245]

Vulnerabilities and consequences of undue pressure on decentralized elected representatives

The 2024 study "A Vulnerable Office: On Subversive Crime and Undue Pressure on Local Elected Representatives (Een kwetsbaar ambt. Over ondermijning en oneigenlijke druk op decentrale volksvertegenwoordigers)" focuses on the relationship between (organised) crime and local elected representatives. Respondents indicated that they observed noticeable behaviour. However, due to a lack of insight into the motives, they found it difficult to interpret this behaviour. Therefore, it is certainly not the case that these behaviours or characteristics are necessarily problematic in and of themselves for functioning properly as an elected representative. Respondents identify vulnerabilities in the fact that local elected representatives provide an entry point to administrators and civil servants, and that third parties can facilitate such access. Nevertheless, most primarily warn against subversive crime and undue pressure on civil servants and members of the executive board, such as aldermen.

Risks of undue pressure on elected representatives within their own social and professional networks are underestimated, such as contacts in the neighbourhood, community associations, or with local entrepreneurs. Many elected representatives are unaware of this or pay too little attention to it, they benefit from it, or find it difficult to address this pressure, as this could have consequences for their own position within that community.

The researchers refer to a 'vulnerable office' when it comes to decentralized elected representatives. They are referring to the risks of undue pressure and their vulnerabilities to this, but also to the lack of clarity regarding the scale and the number of cases in which pressure from criminals is involved.

If elected representatives make decisions under undue pressure from third parties, the functioning of the entire local democracy is jeopardized. This can lead to a decline in the effectiveness, efficiency, and legitimacy of local government; trust in the administration is undermined, potentially resulting in a decrease in participation and a deterrent effect on individuals wanting to become elected representatives themselves.[248]

Box 7.7

Manipulation of the judiciary enables criminal networks to delay or sabotage judicial procedures, threaten officials, or obtain information on criminal investigations. The assassination of crime journalist Peter R. De Vries in 2021, who was also an advisor to a state witness, was according to the OM intended to spread fear among the population of the Netherlands, and the OM characterized the murder as terrorism.[249]

Example of sharing information with contacts in criminal circles

The OM reported in March 2025 that the Rijksrecherche (the Dutch National Police Internal Investigations Department) arrested an employee of the Amsterdam district court. An investigation by the Rijksrecherche indicates that the woman had presumably requested information from court systems over a prolonged period and shared this for payment with contacts from the criminal world. Dozens of printouts containing personal data were seized upon her arrest.[254] In March 2026, the proceedings were still ongoing.

Box 7.8

Municipalities are vulnerable to infiltration and influence by criminal networks

An investigative report shows how vulnerable municipalities can be to infiltration and influence by criminal networks. RTL journalists identified more than 100 integrity breaches of in the period 2020-2022, based on information requested from 342 municipalities. These violations range from leaking confidential information to bribery and fraud. A striking example concerns an official who was suspected of stealing 640,000 euros and nevertheless was able to be seconded to another municipality without any difficulty. The Rijksrecherche warns that administrative security is insufficient in many municipalities.[255]

Box 7.9

Criminal networks have a strategic interest in structurally manipulating the executive power. This allows them, for example, to gain access to information or exert influence on policy, licensing, supervision, and operations of organisations such as the Netherlands Police, FIOD, Dutch Tax Administration, and OM. Furthermore, the manipulation of executive bodies in other countries can provide structural advantages for criminal networks operating in the Netherlands. For instance, the use of various identity documents is important for shielding. In this way, criminals leave no direct traces when they have to travel abroad for their criminal activities. A Dutch criminal possessed five false identities and also posed as a Macedonian and a German. The German passports were allegedly provided by a former official from Cologne (Germany).[250]

Criminal networks also have a strategic interest in influencing and manipulating the media and journalism. Some crime journalists in the Netherlands are being threatened. This culture of fear, amplified via digital channels, can lead to reluctance among journalists and researchers[251] and limits the independent exercise of journalism. As a result, press freedom may come under structural pressure.

Attempted criminal manipulation of reporting

According to the AIVD, criminals regularly try to ensure that criminal competitors get public attention in the hope that they will thus attract the attention of the Netherlands Police and the justice system. "Such manipulation is dangerous for journalists, because members of criminal networks may view them as an extension of rivals or of the investigation services. This increases the risk that they are seen as legitimate targets. The threat of violence against journalists can also lead to (self-) censorship. If press freedom is restricted in this way, it harms the democratic rule of law."[256]

Box 7.10

"The AIVD views the intelligence work of criminal networks as a threat to national security. Primarily because it increases their capacity to plan and organise violence against, among others, lawyers, judges, prosecutors, journalists, officials, and politicians. In the interest of the rule of law, people in such professions must be able to carry out their work unhindered and safely. It also harms the legal order if parts of the government are infiltrated by or for criminals. This means that citizens can have less confidence that these organisations are performing their duties properly. This is particularly harmful if these are tasks that are indispensable to the democratic legal order."[257]

7.11 Subversive effects information gathering

Violence and some reasons for it

Slightly more than half (52%) of the victims of an assassination in the period 2016-2023 were killed within their own camp. The "own camp" is defined as those with whom a collaborative relationship existed or for whom assistance or services were provided. The most common motives for assassinating someone internally were non-performance, stealing from their own criminal network, loose lips in the criminal underworld, or talking to the Netherlands Police and the justice system.

According to the Netherlands Police, explosive attacks within the criminal underworld were typically caused by disputes over money or drugs that had disappeared, been stolen, or had been seized by the Netherlands Police.[258]

Box 7.12

Information about opponents is of great importance to criminal networks. Information about them can be found both within the government and in economic sectors. They can obtain information through various activities, which are interchangeable (see section 3.1). According to the AIVD, criminal networks have developed capabilities comparable to those of intelligence and investigation services to gather information on opponents. To do this, they exploit every vulnerability they can find in the legislation, policy, or work practices of government entities and companies.[252] Deficient authorisation, logging, and monitoring, and the insufficient implementation of basic cybersecurity measures constitute vulnerabilities in ICT and information processes. These provide opportunities to obtain necessary information (see also section 3.3.6).

The use of violence or the threat thereof is sometimes seen as necessary in the criminal world when interests are harmed. After all, criminal networks cannot go to court, and failing to respond to retaliation from rivals would carry consequences for their credibility in the future (see section 2.3).

A successful approach by the government can unintentionally contribute to violence. Much of the mutual violence between criminal networks in the past originated from, for example, the seizures of drug shipments. The Dutch Safety Board (Onderzoeksraad) stated in 2023 that the consideration of whether or not to deploy a state witness places the government before a dilemma. Through such deployment, the government can tackle organised crime more effectively and improve safety within society. At the same time, a dangerous situation arises for, for example, family members of the state witness and persons who assist them in a professional capacity. In 2018, the brother of a state witness was murdered. In 2019, the lawyer of the same state witness, and in 2021, crime journalist Peter R. De Vries, who was also an advisor to the same state witness., were assassinated. "At the time of the attacks on their lives, all three victims were monitored by the Monitoring and Protection system (stelsel Bewaken en Beveiligen) [...] due to a threat which, according to the available information from the OM and the Netherlands Police, originated from serious organised crime. According to the OM and the Netherlands Police, in all three cases, this threat originated from the same criminal network [....]." The threat had arisen as a result of the negotiation of and the entering into a state witness deal. The Dutch Safety Board stated that the attacks caused social unrest and are seen as an attack on the rule of law.[253]

Criminal networks employ symbolic or high-profile (public) assassinations to sow fear. By spreading threats, propaganda material, and violent images via social media, news, and other digital channels, they reinforce their reputation for ruthlessness. Furthermore, due to AI developments, new opportunities arise for criminal networks to create fake images of assassinations in order to intimidate citizens and competitors. Competitors may, in turn, respond to this and contribute to the perception of the normalisation of violence.

The threat posed by the use of physical violence by criminal networks can affect officials in the performance of their duties. When specific organisations or professional groups are faced with (the threat of) violence, the attractiveness of those positions decreases, making it more difficult to fill those positions.

The distinction between isolated incidents and structural manipulation can only be determined with a comprehensive overview of events. The dark number of at least criminal interference, including corruption, infiltration, and threats, is substantial: there is a lack of uniform and accessible registration. Insufficient awareness of the scale and opportunities for abuse, vulnerabilities, and the harm of structural manipulation may play a role in this (see section 4.2).

In addition to the more common counterstrategies, criminal networks will certainly not shy away from innovating them: after all, they are agile. Consider the use of unmanned systems such as drones, digital platforms and AI (see section 5.1), and developments in encrypted communication. With these, they can, in innovative ways, for example, evade government operations, gather information, carry out assassinations, and destroy evidence. They can also learn from the war against Ukraine when it comes to the use of drones, for example. Developments are moving extremely fast, while laws and regulations, supervision and control cannot always keep up. This enables criminal networks to better protect their interests.

Possible example of the signalling function of violence

On October 3, 2025, an Albanian cocaine smuggler was found dangling from traffic signs along the Brussels Ring (Belgium). Although the possibility of suicide was not completely ruled out, it was assumed that the hanging was a warning and possibly related to the loss of a shipment of coke.[259]

Box 7.13

Impact of the threat from organised crime on the Netherlands Police

An exploratory study from 2024 into the impact of threats from organised crime on police officers and their loved ones shows that both officers in investigation and in basic teams encounter this. Nearly a quarter of these officers state that they have experienced this themselves. Approximately 10% of the officers who have not experienced a threat themselves estimate the probability as (very) high that this will happen in the future. Despite this result, most police officers do not experience a -conscious- negative impact from the threat, and the most frequently mentioned form of impact is actually increased motivation. Perceived threat can, however, also lead to diminished mental well-being and changes in behaviour. The study highlights numerous examples showing that suspects have access to personal information about police officers, such as addresses, license plates, or the addresses of schools attended by the officers' children.[260]

Box 7.14

Remote control via digital channels

Clients domestically and abroad hire young Dutch nationals to carry out kidnappings, torture, and assassinations. This form of 'crime-as-a-service' often operates via social media, where young people are recruited in exchange for payment or debt forgiveness. The perpetrators typically have no direct relationship with the victims or the underlying conflicts. They travel abroad on demand, commit extreme violence, record the act on video as proof for the clients, and subsequently return. These videos function as a system of control and enforcement within the networks and enable the remote provision of evidence. [261]

Box 7.15

Assessment

It is conceivable that decision-making and the functioning of institutions are (in)directly influenced by manipulation. Murders in Italy in the 1990s and examples in some South American countries show that organised crime impairs the functioning of a society. In the Netherlands, there are also concerning examples of the use of violence to send a message to criminals, the government and/or society. The murder of a state witness's brother in 2018, of the same state witness's lawyer in 2019, and the murder of a crime journalist, who was also an advisor to that state witness, caused a shock in the Netherlands at the time. Media reports in 2022 regarding a possible criminal threat against the Crown Princess and the then-Prime Minister Rutte, and the plot to kidnap the then-Belgian Minister of Justice, also illustrate how far some criminals are willing to go. In any case, under certain circumstances, criminal networks have a strategic interest in the structural manipulation of (parts of) society. Especially when the interests of criminal networks grow and come under pressure, the importance of manipulation increases and they actively engage in conflict with their opponents, including officials of the rule of law. Conversely, subtle forms of manipulation present fewer risks for criminal networks than 'heavy artillery'. Precisely the aforementioned assassinations have led to numerous measures to intensify the approach to organised crime.

Several system vulnerabilities make the detection of (indications of) manipulation complex. These relate to limitations in the approach to combat organised crime and in laws and regulations, more specifically limitations on the exchange and processing of information concerning such indications. This also includes low awareness of, for example - but not exclusively - corruption vulnerabilities, the lack of or minimal reporting of corruption or recruiting, and/or a closed culture as a result of which corruption is less likely to be noticed or reported. Technological developments offer opportunities, more specifically through, for example, the use of drones in the application of violence, the development of digital platforms for issuing assignments, and AI for generating advanced disinformation.

Structural manipulation undermines national security. This primarily concerns the security interests of economic security, social and political stability, and to some extent territorial security and physical security. In this way, manipulation neutralizes the functioning of the rule of law, or in extreme cases, the rule of law even becomes instrumental in promoting the interests of organised crime. This leads to serious harm to the vitality of and trust in political-administrative infrastructures. Through manipulation, the government may lose control over economic sectors and/or neighbourhoods. This affects the national security interests of territorial security, more specifically the so-called impact criterion "Impairment of the integrity of the (Dutch) territory" due to loss of control. Manipulation also leads to social harm by undermining horizontal and vertical social cohesion. In the case of psychological and physical violence, it also has a negative impact on the objective and subjective safety of citizens or employees of organisations and, in extreme cases, can lead to deaths and injuries. This affects the national security interests of physical security. Harm also arises to economic infrastructures through the erosion of trust, the neutralisation of rule-of-law safeguards, and the growth of illegal positions of power.

Furthermore, damage is caused to the international reputation of the Netherlands. This affects the national security interests of territorial security, more specifically the so-called impact criterion "impairment of the integrity of the international position of the Netherlands". After all, structural manipulation reduces the attractiveness of the Netherlands for investments and economic activities and can also lead to a reduced willingness for international cooperation in tackling organised crime.

7.5 Threat: Illegal proceeds find their way into society through the diverse use of financial channels

Criminal networks have various options for using financial channels, through which illegal proceeds become intertwined with legal ones and find their way into society. Criminal networks face a double challenge when it comes to 'financial management'. They must legitimize financial flows, on the one hand to secure the money and on the other hand to be able to use it while avoiding supervision and investigation. In doing so, they make use of traditional banking infrastructures, new, often global and digital (financial) infrastructures, and underground banking. The interaction and integration of various systems – such as the adoption of cryptocurrencies by underground bankers[262] – make it possible to combine both traditional and new financial channels. This diversification enables criminal networks to set up increasingly sophisticated money laundering schemes. At the same time, this interplay increases the complexity of enforcing laws and regulations.

Underlying interest for organised crime

Criminal networks have a significant interest in using diverse financial infrastructures, as this enables them to continue their business operations, conceal and spend illegal proceeds, and build up legal assets, and thereby exercise influence and establish or strengthen positions of power. The ever-increasing fragmentation of the (digital) payments landscape offers ample opportunities to 'benefit' from the obtained proceeds and spread risks by staying under the radar of gatekeepers and the government.

Infrastructures and vulnerabilities exploited by criminal networks

Despite strict laws and regulations, criminal networks still make use of the regular payment system. Opportunities to make use of it continue to exist, including indirectly, for example through facilitating legal entities. In addition, new entities are often established with complex international and legal structures, among other things to enable so-called 'trade-based transactions'. Specifically, a development is observed where numerous companies are established with the sole purpose of facilitating money laundering and committing fraud.[263] In the Netherlands, the establishment of a company is explicitly organised in a highly accessible manner. Registration in the Trade Register (Handelsregister) is deliberately designed to be simple and accessible, making it possible to start a company with limited barriers.[264] Not only can new entities be established relatively easily, but the ultimate owner can also remain hidden. All of this puts great pressure on gatekeepers who must investigate these companies and ultimate owners.[265]

Additionally, informal financial infrastructures meet the needs of criminal networks for payments, for example through underground banking. Criminal underground banking is a world of its own. It is extensive, professional, involves large sums of money, and transactions occur at a high pace. It is estimated that approximately three-quarters of all international drugs trafficking is facilitated by criminal underground banking. In drugs trafficking, the focus is primarily on cash, and for every commodity flow there is a corresponding financial flow. Underground banking plays a major role in this, but has since also become involved in other services or investing in criminal projects.[266] Providers thus cater to the needs of criminal networks. Underground banking has evolved into a larger, faster, and more dynamic network than in the past, with more complex methods and a hybrid structure in which physical, digital, and symbolic forms of value converge.

The use of cryptocurrencies continues to offer opportunities for criminals. Cryptocurrencies operate on decentralized blockchain networks, allowing transactions to take place without a central intermediary such as a bank. Within this system, decentralized financial applications have also emerged, where financial services are executed via smart contracts. Consequently, transactions are more difficult to monitor or intercept, and assets can be transferred relatively anonymously.[267]

Mixed forms of financial transactions
In practice, techniques are combined: underground bankers make use of corporate structures, money laundering schemes such as the Cash Compensation Model, trade-based money laundering and cryptocurrencies for the international transfer of value.[271] Although other stores of value such as gold or luxury goods are seen less frequently, it is likely that in the future underground bankers will more often engage in value-driven transactions, for example via (digital) art. This allows criminal networks to move financial flows and value outside the sight of authorities and maintain access to resources.

Box 7.16

Transactions via virtual platforms
In March 2021, a digital art collage (NFT) was sold for 69.3 million euros. It was not a physical painting or object, but a purely digital work of art that could only be traded via NFT. The value of such a digital asset is determined by a 'token price', or in other words, whatever a fool is willing to pay for it. These environments offer little transparency regarding identity and trade, while substantial values are transferred. Because there is hardly any oversight or regulation, these platforms are ideally suited for concealing large financial flows and cross-border transactions.[272]

Box 7.17

Other infrastructures also make it possible to transfer digital assets outside of banks and regulators, such as NFTs[268]: unique digital tokens that record ownership of an object. NFTs can be traded via platforms, for example in the case of digital art or virtual commodities. Direct transfers between users offer limited oversight, because the identity of those involved is not always verified.

The oversight of cryptocurrency (providers) faces major challenges, including continuing to respond to new developments and associated opportunities for abuse. Although rules now exist, investigation and oversight depend on private parties and international cooperation, which is often slow or limited. Criminal networks take advantage of this by choosing providers - whether malicious or not - who cooperate little, or by moving to countries where requests for legal assistance are not honoured. Due to the cross-border nature of cryptocurrencies, providers are mobile and not tied to a specific location, which complicates oversight.[269] Developments, such as the societal acceptance of crypto, for example through payment cards and stablecoins, furthermore make the use of digital currencies increasingly accessible and user-friendly. As a result, criminal networks can more easily use their illegally obtained money for their business operations or invest in markets such as real estate and gold.[270] Feedback on the draft version of the STAN showed that different views exist regarding possibilities for the oversight of cryptocurrency (providers). This is, in any case, an illustration of the complexity.

We can now speak of fragmented financial infrastructures. This provides opportunities for criminal networks to limit risks. Developments, particularly in digital financial infrastructures, are moving so quickly that laws and regulations struggle to keep up, and the use of these infrastructures can often – whether or not for an extended period – remain under the radar of law enforcement. Gatekeepers such as banks, notaries and accountants see only a part of the bigger picture. Because traditional gatekeepers lack the full picture, the barriers designed to prevent the mixing of illicit and legal proceeds are under pressure.

Some crypto exchanges process criminal money
Large cryptocurrency exchanges continue to process significant amounts of criminal money despite pledges of stricter controls. Research shows that in two years, at least $28 billion in illegal funds have passed through platforms used by criminal networks, North Korean hackers, and scammers to launder crypto. A platform still receives suspicious money flows, including from US-sanctioned actors, and has closed large deals while law enforcement against crypto platforms has weakened. The financial significance of transactions makes these exchanges attractive for criminal activities.[273]

Box 7.18

Limitations in the approach to criminal money
Seizing criminal money is more complex than ever, said the national coordinating public prosecutor for tackling criminal money flows in April 2025. "Municipalities are sometimes uneasy about real estate, when you know something is wrong, but it is not clear who the owner is. Ingenious, often international money laundering schemes are set up, and sometimes you have as many as 400 legal entities at one address. It is very easy to register with the Chamber of Commerce (Kamer van Koophandel). Sometimes what you want to seize feels within arm's reach, but you are held back by the burden of proof, poor international cooperation, and legislation. Organised crime has so many opportunities, and we are hitting the limits of the rule of law."[274]

Box 7.19

Assessment

Criminal networks are already making extensive use of diverse financial channels. After all, they have an interest in diversifying financial channels and continue to respond to new developments to achieve their goals and limit risks. For laws and regulations and their enforcement, it is not only a challenge to keep up with developments, but also to take into account the often global nature of these channels, the complexity of money laundering methods, and limitations in data sharing. The ease with which criminals can establish (complex structures of (inter)national) legal entities constitutes an additional vulnerability.

Illegal proceeds that find their way into society undermine national security, in particular economic security and social and political stability. Through the intertwining of illegal and legal money, criminal networks gain influence and establish a position of power within economic and social infrastructures. This undermines the vitality of and trust in economic infrastructures, for example through the distortion of competition, and negatively affects social cohesion. When criminal networks are able to live lavishly and gain influence in sectors and neighbourhoods, the perception arises that participating in crime is attractive. Furthermore, it goes without saying that illegal money that remains underground contributes to influence within the criminal world and, for example, can be used to carry out assassinations or can be invested in criminal projects. Damage to the international reputation of the Netherlands is also plausible. This affects the national security interests of territorial security, more specifically the so-called impact criterion "undermining of the integrity of the international position of the Netherlands".

7.6 Threat: Cumulative harm due to the intertwining of criminal actors with state or ideological actors

The intertwining of activities of state actors*, ideologically motivated actors including terrorists, and criminal actors results in cumulative harm to society. Activities of each of these types of actors already lead to harm, and certainly so when they assist one another through cooperation or the provision of services. In the current geopolitical context, it is attractive for state actors to deploy criminal networks as an 'instrument' in hybrid warfare.** Conversely, criminal networks can benefit when they provide services or products to state actors. Well-known examples of cooperation between state and criminal actors are those between Russian state actors and Russian cybercriminals for the execution of cyberattacks.[275] This may also involve the outsourcing of activities. Examples of this include having assassinations carried out in Western countries by criminals on behalf of Iran.[276] (Un)conscious forms of intertwining between criminal and ideologically motivated actors can also offer mutual benefits. Furthermore, there are examples of terrorist networks that have engaged in organised crime, such as the IRA, PKK and FARC, some of which continue to do so.

* State actors are official bodies or representatives of a state acting under governmental authority. In this context, this may for example involve unwanted foreign interference.

**It concerns conflict between states that largely takes place below the legal threshold of open armed conflict, involving the integrated use of means and actors to achieve specific strategic objectives. Examples include sabotage of railway infrastructure or the spread of disinformation.

Underlying interest for organised crime

State actors possess knowledge, capabilities and resources that are valuable to criminal networks. These include weapons, identity documents and the provision of safe havens when governments are pursuing them. Conversely, criminal networks possess professional capabilities or resources in the Netherlands, such as complex money laundering schemes, intelligence and violence capabilities, technical means and expertise, or control over logistical and smuggling routes. They can offer these to state actors who wish to carry out (or have carried out) undesirable and/or illegal activities in the Netherlands. For example, state actors employ cyberattacks to achieve their political,

State actors utilize criminal networks
In the "Insider Risk Trend Report 2026" by Signpost Six, it is stated that state actors use criminal networks to carry out operations, such as sabotage or the spread of disinformation. Criminal networks can carry out activities for state actors, including the recruitment or corruption of insiders such as employees, customers, or partners to gain access to systems, facilities, or information. Both the state actor and the criminal network benefit from this. This practice significantly blurs the line between an action employed by a state and an action employed by a criminal. The tactics of criminal networks are generally of a different nature than the usual tactics of state actors. Indeed, the tactics of criminal networks are often accompanied by intimidation, coercion, or violence.[284]

Box 7.20

military and/or economic objects with the assistance of criminal actors. In this way, state actors (covertly) pursue their interests without crossing the legal threshold of an armed conflict. Furthermore, state actors can deny involvement when they deploy criminals.[277]

Not only can state actors benefit from organised crime; the same applies to ideologically motivated actors, such as terrorist or extremist groups. This provides opportunities for criminal networks, primarily in the form of facilitation or service provision. However, the relationships that result from this do not necessarily involve conscious or ideologically driven cooperation. These can range from purely transactional service provision, such as the supply of commodities or logistical support in exchange for payment, to more structural forms of coordination and cooperation. In some cases, terrorist actors are also engaged in organised crime themselves. For example, the African cell of the Lebanese terrorist group Hezbollah is active in drugs trafficking.[278]

In the Dutch and broader European context, active and conscious collaboration between criminal networks and terrorist actors is less likely. Criminal networks are generally focused on maximising financial gain while operating as inconspicuously as possible. Terrorist actors, on the other hand, often strive for societal disruption or political influence driven by an ideological motive. Explicit and demonstrable cooperation with terrorist actors would entail significant risks for criminal networks. After all, the fight against terrorism is a high priority for governments. Association with terrorism can lead to an intensification of investigation and prosecution. From a criminal perspective, this is unfavourable.

That a conscious alliance is less likely does not, however, mean that forms of facilitation or business interaction are excluded. Given the opportunistic and profit-driven nature of criminal networks, it is conceivable that they provide services when this is financially attractive and the risks are deemed manageable. For example, in Greece, members of criminal networks were paid for their contribution to attacks, without sharing the same ideological convictions.[279] In such cases, it is more a form of crime as a service than ideologically motivated cooperation. It also appears that firearms used in terrorist attacks were obtained via criminal networks, through criminal contacts that had already been established.[280] The firearms used in the attack on the Bataclan in Paris, for instance, were obtained via Dutch criminals.[281]

Unconscious or indirect facilitation of terrorist or other ideological actors also cannot be ruled out. It is plausible that criminal networks do not always have, or seek to have, insight into the underlying motives of their customers. For activities such as human smuggling, financial services, or arms trafficking, purely transactional arrangements may occur. Illustrative of this are the possibilities the dark web offers for arms providers; it is relatively easy to obtain a weapon via this route[282], without the seller knowing what the buyer intends to do with the weapon. The service provider therefore does not necessarily have to be mindful of the ultimate objective. In addition, both ideological and criminal actors can make use of the same criminal infrastructures, without necessarily being aware of each other's involvement. This applies, for example, to underground banking, where it appears that cryptocurrencies are used both for terrorism financing and for the financial flows of criminal networks.[283]

Infrastructures and vulnerabilities exploited by criminal networks

Geopolitical developments are increasing political tensions worldwide and thereby influencing opportunities for criminal networks (see section 5.2). For example, criminal networks are suitable for hybrid operations within economic, political-administrative, and social infrastructures. In the context of current geopolitical tensions, it is likely that hybrid warfare will intensify and that cooperation between criminal networks and geopolitical actors will further increase. In the Netherlands, the use of criminal networks is most likely aimed at obtaining information to apply psychological or physical violence, or for exploiting logistical and financial infrastructures.

Logistical infrastructures can, for example, be used to circumvent sanctions. Financial infrastructures can be used for payments to perpetrators. System vulnerabilities such as limited international coordination and fragmented information (sharing) can contribute to such criminal networks or service provision going undetected. On the other hand, the threat posed by state actors specifically has the explicit attention of, for example, the AIVD. Furthermore, the intertwining of ideologically driven and criminal actors may also go undetected due to the aforementioned system vulnerabilities, with the caveat here as well that the approach to ideological actors is high on the agenda of, for example, the AIVD.

Digital platforms make it easier to establish contacts between different actors. These platforms also offer opportunities for a certain degree of anonymity, while oversight faces complications (see further in section 5.1).

Example of possible cooperation with state actors

According to the AIVD, the level of intelligence-gathering and violent capabilities of Dutch criminal networks makes it more attractive for state actors that threaten the national security of the Netherlands to collaborate with them. This may include intelligence operations, acts of sabotage, or assassination attempts.[285]

The "Threat Assessment of State Actors (Dreigingsbeeld Statelijke Actoren) 2025" states that Iran has criminal connections in the Netherlands that can carry out activities in the Netherlands. These involve more experienced criminal networks. These could, for example, be deployed against Israeli targets. It also states: "Since the beginning of 2024, various attacks have been carried out on Israeli targets in Sweden and Denmark. In Sweden, these are said to be attacks by juvenile offenders whose gang leaders were recruited by Iran."[286]

Box 7.21

Examples of possible cooperation with ideological actors

A Dutch man, previously convicted of weapons trafficking, was suspected in 2025 of participating in a criminal network. The network allegedly adhered to an anti-institutional ideology and was willing to use violence, with the man presumably playing a role in the supply of weapons.[287] The case was still ongoing in March 2026.

Box 7.22

Assessment

In the current geopolitical context, the blending of activities between criminal networks and state actors is already occurring as an instrument for hybrid warfare or for the execution of assassinations of opponents of foreign regimes. Criminal networks can, in turn, gain strategic advantage from cooperation or service provision.

Globally, there are examples where terrorist networks have engaged or are engaging in organised crime. Criminal networks can collaborate with terrorist and/or other ideological actors. As a result, criminal networks are more likely to come to the attention of intelligence and investigation agencies, increasing their exposure to risks. For criminal networks operating in Europe and the Netherlands, unwitting service provision via fluid networks is more likely than active and/or conscious cooperation.

The intertwining of criminal actors on the one hand, and state or ideological actors on the other, amplifies the threat that individual actors pose to national security. The fact that state and ideological actors pose a threat to national security is evident from the periodic products of the NCTV, such as the "Terrorism Threat Assessment Netherlands (Dreigingsbeeld Terrorisme Nederland)"[288], "CSAN"[289], the joint product of the NCTV, AIVD and MIVD "Threat Assessment of State Actors"[290], and the annual reports of the AIVD[291] and MIVD[292]. Intertwining with criminal networks can reinforce the strengths of the actors involved while offsetting their weaknesses. Infrastructures are then utilised not only for criminal purposes, but also for geopolitical or ideological objectives.

The cumulative harm and impairment of national security interests depend heavily on the specific form this interconnection takes. Potentially, all security interests may be compromised.

8

Appendix 1
Account of development

A1.1 Development phases

The Strategic Knowledge Centre on Subversive Crime (SKC) started the process for the creation of the Subversion Threat Assessment Netherlands (STAN) in the spring of 2025. The Directorate-General for Subversive Crime of the Ministry of Justice and Security (DGO), acting as the coordinating client, commissioned the SKC for this threat assessment in 2025.

The development of STAN consisted of the following phases:

1. **Gathering and processing information:**
   At the end of March 2025, the SKC requested information from various organisations and partnerships that play a role in the integrated approach to subversive and organised crime. There was a massive response to this request, and we received around 150 documents from more than 20 types of organisations. We also collected documents from other sources throughout the entire process.

2. **Analysis:**
   We have studied, summarized (from the specific focus of the STAN), and analysed the obtained and gathered documents. Based on this study and analysis, we organised four expert meetings in July 2025 with experts from various public and private organisations. Based on those findings and additional documents, we continued our analysis. The analysis centred on the various variables that form our starting point, namely: subversive activities, infrastructures, system vulnerabilities, subversive effects, and threat. In October 2025, we also held an “Expert meeting science” and an “Expert meeting legal profession,” in which the focus was on the discussion of threats.

3. **Drafting.**
   Partly in parallel with the analysis phase, draft chapters were written by separate (teams of) authors. In some cases, additional conversations took place for further elaboration.

4. **Validating draft.**
   At the end of January 2026, a broad group of experts was asked to provide feedback on a first draft of the STAN.

5. **Making up the final draft.**
   After processing the feedback and the final editorial review, the final draft has been drawn up.

A1.2 Partner involvement

Within the first two phases, a total of more than 75 organisations have been involved in various ways. They provided information and also participated in expert meetings, in which knowledge, experience and perspectives were shared to collectively provide insight into issues.

This involvement came from diverse domains, including national and regional partnerships in the field of security and subversive crime, municipalities and umbrella organisations, knowledge and research institutions, executive and law enforcement organisations of the Government of the Netherlands, regulators, and banks. Additionally, various trade and interest organisations such as transport, agriculture, real estate, recreation and the business community were involved, as well as parties from the care and security chain and legal professionals.

A draft of the STAN was sent to more than 60 contact persons from organisations for validation at the end of January 2026. In this phase, they were able to provide feedback down to the sentence level. 43 contact persons provided feedback in various levels of detail. This feedback has been incorporated into the final draft. The involved organisations came from diverse domains: national and regional partnerships in the field of security and subversive crime, municipal and umbrella organisations, knowledge and research institutions, executive and law enforcement organisations of the Government of the Netherlands, regulators, and banks. In addition, trade and interest organisations from sectors including transport, agriculture, real estate, recreation, and the business community were involved, as well as parties from the care and security chain and legal professionals.

A1.3 Methodological explanation

The creation of the STAN began with the development of a conceptual model. In this model, the key concepts and the interconnections between them have been elaborated. Additionally, the principles, as well as the research questions and scope, have been set out (see sections 1.3 and 1.4 for the essence thereof). The choices underlying the conceptual model were made in close consultation with the commissioning party. The model was presented during several meetings.

When collecting sources, a distinction was made between reports, articles and other grey literature (hereinafter: documents), news reports and scientific literature. For documents, the selection criterion was that they must have been published after the first of January 2023. In some cases, older documents were included, when both the requested organisation and the internal analysis indicated that these were considered relevant. Additionally, the snowball method was used, whereby additional relevant sources were identified via the references of already selected documents, with specific attention to gaps in the existing documentation.

The selection of documents was conducted using a step-by-step approach. First, the introduction, table of contents, and conclusion were scanned to assess relevance. If a document appeared to be relevant, it was read in full and systematically summarized.

A document was considered relevant when it related to organised crime within the Netherlands and (as expected) contained information on the core concepts of the conceptual model (activities, infrastructures, system vulnerabilities, effects, and DESTEP developments, even if these had an international context). The summary was prepared based on these core concepts.

News reports were collected over the period from July 2024 until December 2025. These reports were scanned for alignment with the core concepts of the conceptual model. Where similarities were found, they were included in the analysis. Additionally, illustrative cases and new developments from abroad were included where relevant to the Dutch context. In a few specific cases, reports from the period December 2025 to March 2026 were also included.

For the scientific literature, the snowball method was once again applied, supplemented by suggestions from experts. Additionally, targeted searches were conducted to validate or refute specific information. Scientific literature was not a primary focus, as it often looks back and the data used is often less current, whereas the threat assessment is future-oriented. This literature was primarily used to substantiate characteristics of criminal networks and organised crime.

9

Appendix 2

References

References

1 Nishani Ranaweera, ‘Beyond Numbers: Embracing the Depth of Qualitative Research in Criminology’, 2024.

2 Jerôme Lam Ronald van der Wal Nicolien Kop, ‘Sluipend gif. Een onderzoek naar ondermijnende criminaliteit’, Politieacademie, 2018, p. 20.

3 Voor de samenhang tussen georganiseerde criminaliteit, ondermijnende criminaliteit en ondermijning: zie Jerôme Lam Ronald van der Wal Nicolien Kop, ‘Sluipend gif. Een onderzoek naar ondermijnende criminaliteit’, Politieacademie, 2018, p. 20.

4 Jerôme Lam Ronald van der Wal Nicolien Kop, ‘Sluipend gif. Een onderzoek naar ondermijnende criminaliteit’, Politieacademie, 2018, p. 20.

5 Politieacademie, ‘Trefwoord ‘Crimineel samenwerkingsverband’’, https://thesaurus.politieacademie.nl/Thesaurus/Term/4328 geraadpleegd op 10-12-2024.

6 Enquêtecommissie Opsporingsmethoden, ‘Bijlage VII: Eindrapport onderzoeksgroep Fijnaut’, 1996, p. 24-25.

7 Rijksoverheid, ‘De Veiligheidsstrategie voor het Koninkrijk der Nederlanden’, 03-04-2023, p. 11, www.rijksoverheid.nl/documenten/publicaties/2023/04/03/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden.

8 Europol, ‘Decoding the EU’s most threatening criminal networks’, 11-10-2024 www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks#downloads; Klaus von Lampe, ‘Transnational Organised Crime in Europe’, 01-2014, in Transnational Organised Crime: An Overview from Six Continents, Albanese en Reichel (Reds.), www.researchgate.net/publication/294820990_Transnational_Organised_Crime_in_Europe; Letizia Paoli, The paradoxes of organised crime, 2002, www.researchgate.net/publication/225889684_The_Paradoxes_of_Organised_Crime; Koen van der Zwet, Ana I. Barros, Tom M. van Engers en Peter M.A. Sloot, ‘Opportunistic Organisation of Illicit Supply Chains’, 16-05-2025, https://link.springer.com/content/pdf/10.1007/s10940-025-09613-x.pdf.

9 Politie, ‘Samenwerken en uitbesteden: georganiseerde misdaad in beeld. Fenomeenbeelden 2024’, 09-2024, www.politie.nl/binaries/content/assets/politie/onderwerpen/publicaties/2024/317712e8-1458-4b4c-bb2c-740f53089391.pdf; Dirk J. Korf, Simone J. Luijk en Miranda E. de Meijer, ‘Criminele samenwerkingsverbanden: Ontwikkeling in aanpak en duiding van effectiviteit’, 2018, https://repository.wodc.nl/bitstream/handle/20.500.12832/2285/2723A_Volledige_Tekst_tcm28-365539.pdf?sequence=2&isAllowed=y; Europol, ‘Decoding the EU’s most threatening criminal networks’, 11-10-2024 www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks#downloads; Klaus von Lampe, Transnational Organised Crime in Europe, 01-2014, in Transnational Organised Crime: An Overview from Six Continents, Albanese en Reichel (Reds.), www.researchgate.net/publication/294820990_Transnational_Organised_Crime_in_Europe.

10 Martin Bouchard, ‘Collaboration and boundaries in organised crime: A network perspective’, 01-2020, www.researchgate.net/profile/Martin-Bouchard-5/publication/341214324_Collabouration_and_Boundaries_in_Organised_Crime_A_Network_Perspective/links/5eb42dae299bf152d6a35d9d/Collabouration-and-Boundaries-in-Organised-Crime-A-Network-Perspective.pdf?origin=journalDetail&_tp=eyJwYWdlIjoiam91cm5hbERldGFpbCJ9&__cf_chl_tk=8U.eG4nfxXotogH6q9miAB.p8ZoW_gbgxdvwpTsUHEo-1762162112-1.0.1.1-teuSkdPCv9heMrk1G4DnLeBifDxK_djPpMXVdu2cGqU; Letizia Paoli, The paradoxes of organised crime, 2002, www.researchgate.net/publication/225889684_The_Paradoxes_of_Organised_Crime; Edward Kleemans en Vere van Koppen, Organised Crime and Criminal Careers, 2020, www.researchgate.net/publication/339084964_Organised_Crime_and_Criminal_Careers.

11 Europol, ‘Decoding the EU’s most threatening criminal networks’, 11-10-2024 www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks#downloads

12 Europol, ‘Decoding the EU’s most threatening criminal networks’, 11-10-2024 www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks#downloads

13 C.A.J. van den Eeden, R.A. Roks, M.V. van Koppen, J.H. Goes, S.J. van Deuverenen L.K. Krijger, ‘Georganiseerde criminaliteit in Nederland: cocaïnesmokkel en liquidaties – Zesde rapportage op basis van de Monitor Georganiseerde Criminaliteit’, 2026.

14 Edward R. Kleemans en H.G. van de Bunt, ‘The social embeddedness of organised crime’, 03-1999, www.researchgate.net/publication/260460230; Edward Kleemans en Vere van Koppen, ‘Organised Crime and Criminal Careers’, 2020, www.researchgate.net/publication/339084964_Organised_Crime_and_Criminal_Careers; Henk van de Bunt, Dina Siegel en Damián Zaitch, The Social embeddedness of Organised Crime, 12-2013, https://dspace.library.uu.nl/bitstream/handle/1874/307660/2014_Social_Embededdness.pdf?sequence=1; Klaus von Lampe, Transnational Organised Crime in Europe, 01-2014, in Transnational Organised Crime: An Overview from Six Continents, Albanese en Reichel (Reds.), www.researchgate.net/publication/294820990_Transnational_Organised_Crime_in_Europe.

15 Edward R. Kleemans en H.G. van de Bunt, ‘The social embeddedness of organised crime’, 03-1999, www.researchgate.net/publication/260460230; Edward R. Kleemans en Christianne J. de Poot, ‘Criminal Careers in organised Crime and Social Opportunity Structure’, 2008, www.academia.edu/21006439/Criminal_Careers_in_Organised_Crime_and_Social_Opportunity_Structure; Renushka Madarie en Edwin W. Kruisbergen, Traffickers in Transit: Analysing the Logistics and Involvement Mechanisms of Organised Crime at Logistical Nodes in the Netherlands: Empirical Results of the Dutch Organised Crime Monitor, 2020, www.researchgate.net/publication/342110879_Traffickers_in_Transit_Analysing_the_Logistics_and_Involvement_Mechanisms_of_Organised_Crime_at_Logistical_Nodes_in_the_Netherlands_Empirical_Results_of_the_Dutch_Organised_Crime_Monitor; Klaus von Lampe, Transnational Organised Crime in Europe, 01-2014, in Transnational Organised Crime: An Overview from Six Continents, Albanese en Reichel (Reds.), www.researchgate.net/publication/294820990_Transnational_Organised_Crime_in_Europe.

16 Robert A. Roks, Edwin W. Kruisbergen en Edward R. Kleemans, ‘Walls of silence and organised crime: a theoretical and empirical exploration into the shielding of criminal activities from authorities’, 25-01-2022, www.researchgate.net/publication/358104014_Walls_of_silence_and_organised_crime_a_theoretical_and_empirical_exploration_into_the_shielding_of_criminal_activities_from_authorities.

17 Edward R. Kleemans en Christianne J. de Poot, 'Criminal Careers in organised Crime and Social Opportunity Structure', 2008, www.academia.edu/21006439/Criminal_Careers_in_Organised_Crime_and_Social_Opportunity_Structure; Klaus von Lampe, 'Transnational Organised Crime in Europe', 01-2014, in Transnational Organised Crime: An Overview from Six Continents, Albanese en Reichel (Reds.), www.researchgate.net/publication/294820990_Transnational_Organised_Crime_in_Europe; Renushka Madarie en Edwin W. Kruisbergen, Traffickers in Transit: Analysing the Logistics and Involvement Mechanisms of Organised Crime at Logistical Nodes in the Netherlands: Empirical Results of the Dutch Organised Crime Monitor, 2020, www.researchgate.net/publication/342110879_Traffickers_in_Transit_Analysing_the_Logistics_and_Involvement_Mechanisms_of_Organised_Crime_at_Logistical_Nodes_in_the_Netherlands_Empirical_Results_of_the_Dutch_Organised_Crime_Monitor.

18 Renushka Madarie en Edwin W. Kruisbergen, 'Traffickers in Transit: Analysing the Logistics and Involvement Mechanisms of Organised Crime at Logistical Nodes in the Netherlands: Empirical Results of the Dutch Organised Crime Monitor', 2020; Klaus von Lampe, 'Transnational Organised Crime in Europe', 01-2014, in Transnational Organised Crime: An Overview from Six Continents, Albanese en Reichel (Reds.), www.researchgate.net/publication/294820990_Transnational_Organised_Crime_in_Europe; Jan Meus, 'Narco's in Nederland. Van Brabantse pillenboeren tot internationale cocaïnesmokkelaars', 2024.

19 Edward R. Kleemans, 'Organised crime and the visible hand: A theoretical critique on the economic analysis of organised crime', 2012, www.researchgate.net/publication/260493016_Organised_crime_and_the_visible_hand_A_theoretical_critique_on_the_economic_analysis_of_organised_crime; Karin van Wingerde, Lieselot Bisschop en Felix Brongers, 'Onbedoeld Ondermijnen: Verkennend onderzoek naar de wijze waarop de Nederlandse overheid onbedoeld de georganiseerde drugscriminaliteit kan faciliteren', 2023, https://repository.wodc.nl/bitstream/handle/20.500.12832/3266/3297-onbedoeld-ondermijnen-volledige-tekst.pdf?sequence=1&isAllowed=y

20 Voor dat laatste: Mondelinge feedback van Openbaar Ministerie op concepversie.

21 Tommaso Cumunale, Francesco Calderoni, Martina Marchesi, Elisa Superchi en Gian Maria Campedelli, 'Systematic Review of the Social, Psychological and Economic Factors Relating to Involvement and Recruitment into Organised Crime', 2020, https://iris.unitn.it/bitstream/11572/289429/2/Comunale2020_Chapter_SystematicReviewOfTheSocialPsy.pdf

22 Politie, 'Samenwerken en uitbesteden: georganiseerde misdaad in beeld. Fenomeenbeelden 2024', 09-2024, www.politie.nl/binaries/content/assets/politie/onderwerpen/publicaties/2024/317712e8-1458-4b4c-bb2c-740f53089391.pdf.

23 Richard Cloward en Lloyd Ohlin, 'Deliquency and Opportunity', 1959; Antonio Nicaso en Marcel Danesi, 'Symbols and myths in Organised crime: a cultural introduction', 2021; Tommaso Cumunale, Francesco Calderoni, Martina Marchesi, Elisa Superchi en Gian Maria Campedelli, 'Systematic Review of the Social, Psychological and Economic Factors Relating to Involvement and Recruitment into Organised Crime', 2020, https://iris.unitn.it/bitstream/11572/289429/2/Comunale2020_Chapter_SystematicReviewOfTheSocialPsy.pdf; Toine Spapens en Dike van de Mheen, 'Het vestigingsklimaat voor drugscriminaliteit in Nederland', 2022.

24 Richard Cloward en Lloyd Ohlin, 'Deliquency and Opportunity', 1959; Toine Spapens en Dike van de Mheen, 'Het vestigingsklimaat voor drugscriminaliteit in Nederland', 2022.

25 Toine Spapens en Dike van de Mheen, 'Het vestigingsklimaat voor drugscriminaliteit in Nederland', 2022.

26 Richard Cloward en Lloyd Ohlin, 'Deliquency and Opportunity', 1959; Antonio Nicaso en Marcel Danesi, 'Symbols and myths in Organised crime: a cultural introduction', 2021; Tommaso Cumunale, Francesco Calderoni, Martina Marchesi, Elisa Superchi en Gian Maria Campedelli, 'Systematic Review of the Social, Psychological and Economic Factors Relating to Involvement and Recruitment into Organised Crime', 2020, https://iris.unitn.it/bitstream/11572/289429/2/Comunale2020_Chapter_SystematicReviewOfTheSocialPsy.pdf.

27 R.K. Merton, 'Social theory and social structure', 1957.

28 SER, 'Gelijke kansen in het onderwijs: structureel investeren in kansengelijkheid voor iedereen', 06-2021, www.ser.nl/-/media/ser/downloads/adviezen/2021/gelijke-kansen-in-onderwijs.pdf?.

29 Edward R. Kleemans, 'Organised crime and the visible hand: A theoretical critique on the economic analysis of organised crime', 2012, www.researchgate.net/publication/260493016_Organised_crime_and_the_visible_hand_A_theoretical_critique_on_the_economic_analysis_of_organised_crime.

30 Edward Kleemans en Vere van Koppen, 'Organised Crime and Criminal Careers', 2020, www.researchgate.net/publication/339084964_Organised_Crime_and_Criminal_Careers.

31 Edward Kleemans en Vere van Koppen, 'Organised Crime and Criminal Careers', 2020, www.researchgate.net/publication/339084964_Organised_Crime_and_Criminal_Careers.

32 Europol, 'Europol spotlight – the use of violence by organised crime groups', 06-12-2021, www.europol.europa.eu/cms/sites/default/files/documents/europol_spotlight_-the_use_of_violence_by_organised_crime_groups.pdf; Letizia Paoli, 'The paradoxes of organised crime', 2002, www.researchgate.net/publication/225889684_The_Paradoxes_of_Organised_Crime.

33 Klaus von Lampe, 'The Application of the Framework of Situational Crime Prevention to 'Organised Crime'', 2011, www.academia.edu/86279989/The_application_of_the_framework_of_Situational_Crime_Prevention_to_organised_crime

34 Edwin Kruisbergen, R. Roks en Edward R. Kleemans, 'Georganiseerde criminaliteit in Nederland: daders, verwevenheid en opsporing', 2019, https://research.vu.nl/ws/portalfiles/portal/93906299/Cahier_2019_17_Volledige_tekst_tcm28_419615.pdf.

35 Politie, 'Samenwerken en uitbesteden: georganiseerde misdaad in beeld. Fenomeenbeelden 2024', 09-2024, www.politie.nl/binaries/content/assets/politie/onderwerpen/publicaties/2024/317712e8-1458-4b4c-bb2c-740f53089391.pdf; Europol, 'Decoding the EU's most threatening criminal networks', 11-10-2024 www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks#downloads.

36 Europol, 'Decoding the EU's most threatening criminal networks', 11-10-2024 www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks#downloads; Klaus von Lampe, Transnational Organised Crime in Europe, 01-2014, in Transnational Organised Crime: An Overview from Six Continents, Albanese en Reichel (Reds.), www.researchgate.net/publication/294820990_Transnational_Organised_Crime_in_Europe; Politie, Samenwerken en uitbesteden: georganiseerde misdaad in beeld. Fenomeenbeelden 2024, 09-2024, www.politie.nl/binaries/content/assets/politie/onderwerpen/publicaties/2024/317712e8-1458-4b4c-bb2c-740f53089391.pdf.

37 Politie, 'Samenwerken en uitbesteden: georganiseerde misdaad in beeld. Fenomeenbeelden 2024', 09-2024, www.politie.nl/binaries/content/assets/politie/onderwerpen/publicaties/2024/317712e8-1458-4b4c-bb2c-740f53089391.pdf.

38 Europol, 'Decoding the EU's most threatening criminal networks', 11-10-2024 www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks#downloads; Politie, Samenwerken en uitbesteden: georganiseerde misdaad in beeld. Fenomeenbeelden 2024, 09-2024, www.politie.nl/binaries/content/assets/politie/onderwerpen/publicaties/2024/317712e8-1458-4b4c-bb2c-740f53089391.pdf.

39 Europol, 'Decoding the EU's most threatening criminal networks', 11-10-2024 www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks#downloads.

40 Jolijn Krijger en Sacha Vriends, 'Corruptiebrokers: bemiddelaars tussen onderwereld en corrupte ambtenaren', 2023; KPMG, 'Een weerbare belastingdienst. Een onderzoek naar de beheersing van corruptierisico's door de Belastingdienst', 2023.

41 Politie, Samenwerken en uitbesteden: georganiseerde misdaad in beeld. Fenomeenbeelden 2024, 09-2024, www.politie.nl/binaries/content/assets/politie/onderwerpen/publicaties/2024/317712e8-1458-4b4c-bb2c-740f53089391.pdf.

42 AD.nl, 'Geweld op bestelling' overspoelt Europa: meer dan 100 Nederlandse ronselaars in het vizier', 8-12-2025.

43 Genoemd in meerdere gehouden expertsessies.

44 Genoemd in meerdere gehouden expertsessies.

45 Europol, 'The changing DNA of serious and organised crime: EU Serious and Organised Crime Threat Assessment 2025 (EU-SOCTA)', 19-03-2025, www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf; Global Initiative Against Transnational Organised Crime (GI-TOC), 'Evaluating Cocaine Market Interventions, How External Shocks Disruption of Criminal Networks Impact the Cocaine Trade and Social Outcomes', www.globalinitiative.net/wp-content/uploads/2025/02/MASIF-Study-on-Evaluating-Drug-Market-Intervention-FINAL-1.pdf.

46 Parool, 'Zo bindt de Zeehavenpolitie de strijd aan met cocaïnebendes en hun handlangers: 'Er komt hier geen partij drugs binnen zonder corruptie'', 08-06-2024.

47 Zeehaven politie, Havenscan nr. 01: drugssmokkel, 01-2025.

48 C.A.J. van den Eeden, R.A. Roks, M.V. van Koppen, J.H. Goes, S.J. van Deuverenen L.K. Krijger, 'Georganiseerde criminaliteit in Nederland: cocaïnesmokkel en liquidaties – Zesde rapportage op basis van de Monitor Georganiseerde Criminaliteit', 2026.

49 Follow the Money, 'De jaloersmakende slimheid van witwassers', 07-12-2025.

50 Robby Roks et al., 'Grip of in de Greep? Een onderzoek naar de gevolgen van de aanpak van ondermijnende criminaliteit voor de Dienst Justitiële inrichtingen', 2024; Robby Roks, 'Over Voortgezet Crimineel handelen in detentie', 2025 (Podcast Politie # Ondermijning #31.

51 Algemeen Dagblad, 'Justitie slaat alarm over onzichtbare coke: 'Alles wat eerst werkte, lijkt nu zinloos'', 21-01-2026, www.ad.nl/binnenland/justitie-slaat-alarm-over-onzichtbare-coke-alles-wat-eerst-werkte-lijkt-nu-zinloos~ae9027af/

52 RIEC Amsterdam-Amstelland, 'Meerjarenplan 2025-2028', 09-2024; R. Staring, L. Bisschop, R. Roks, E. Breinen H. van de Bunt, 'Eindrapport: Drugscriminaliteit in de Rotterdamse haven: aard en aanpak van het fenomeen', 26-05-2019; Jan Meus, 'Narco's in Nederland. Van Brabantse pillenboeren tot internationale cocaïnesmokkelaars', 2024.

53 MAOC(N), 'Annual Report', 2024; Politie, 'Fenomeenbeeld 2024: Geweld van de georganiseerde misdaad in beeld', 2024; R. Staring, L. Bisschop, R. Roks, E. Breinen H. van de Bunt, 'Eindrapport: Drugscriminaliteit in de Rotterdamse haven: aard en aanpak van het fenomeen', 26-05-2019.

54 C.A.J. van den Eeden, R.A. Roks, M.V. van Koppen, J.H. Goes, S.J. van Deuverenen L.K. Krijger, 'Georganiseerde criminaliteit in Nederland: cocaïnesmokkel en liquidaties – Zesde rapportage op basis van de Monitor Georganiseerde Criminaliteit', 2026.

55 Politie, 'Samenwerken en uitbesteden: georganiseerde misdaad in beeld. Fenomeenbeelden 2024', 09-2024; Strategische milieukamer, 'Dreigingsbeeld Milieucriminaliteit 2024', 2025: 'Fintell Alliance, 'Publiek-privaat samenwerken in het wwft domein'; Europol, 'The changing DNA of serious and organised crime: EU Serious and Organised Crime Threat Assessment 2025 (EU-SOCTA)', 19-03-2025; Europol, 'Decoding the EU's most threatening criminal networks', 11-10-2024; Global Initiative Against Transnational Organised Crime (GI-TOC), Evaluating Cocaine Market Interventions, How External Shocks Disruption of Criminal Networks Impact the Cocaine Trade and Social Outcomes', 02-2025.

56 Openbaar Ministerie, 'Jaaroverzicht criminele geldstromen 2023', 14-05-2024.

57 Europol, 'Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures', 2024

58 SKC, 'Expertmeeting Financieel', 2025.

59 Politie, 'Visie op jonge aanwas in de zware criminaliteit vanuit de onderwereld. "Ze willen allemaal Tony Montana zijn"', 03-2023.

60 Frédéric Ouellet, Martin Bouchard en Valérie Thomas, 'The intangible benefits of criminal mentorship', 2021; Hans Moors en Antonius Spapens, 'Criminele families in Noord-Brabant: Over generatie-effecten in de zware criminaliteit', 2017; T. Spapens, H. Moors, L. de Veen, S. van Nimwegen, R. Bredo, S. Vriendsen C. Jacobs, 'Criminele familienetwerken: Subculturele factoren en clan-achtige kenmerken.', 2025.

61 Politie, 'Fenomeenbeeld 2024: Geweld van de georganiseerde misdaad in beeld.', 2024; AIVD, 'AIVD Jaarverslag 2024', 24-04-2025; Europol, 'European Union Serious and Organised Crime Threat Assessment. The changing DNA of serious and organised crime', 2025; R. Staring, L. Bisschop, R. Roks, E. Breinen H. van de Bunt, 'Eindrapport: Drugscriminaliteit in de Rotterdamse haven: aard en aanpak van het fenomeen', 26-05-2019.

62 GI-TOC, 'Final Report: Evaluating Cocaine Market Interventions: How External Shocks and Disruptions of Criminal Networks Impact the Cocaine Trade and Social Outcomes', 02-2025; R.

Staring, L. Bisschop, R. Roks, E. Breinen H. van de Bunt, 'Eindrapport: Drugscriminaliteit in de Rotterdamse haven: aard en aanpak van het fenomeen', 26-05-2019; Politie, 'Fenomeenbeeld 2024: Geweld van de georganiseerde misdaad in beeld', 2024.

63 Antonius Spapens en Dike van de Mheen, 'Het vestigingsklimaat voor drugscriminaliteit in Nederland', 2022.

64 RIEC Oost-Brabant, 'Meerjarenbeleidsplan RIEC Oost-Brabant 2025-2028', 2024; SKC, 'Expertmeeting advocatuur', 2025.

65 Politie, 'Havenscan Nr. 01. Drugssmokkel', 02-2025; RIEC Zeeland West-Brabant, 'Meerjarenbeleidsplan 2025-2028', 2024; Shanna Mehlbaum, Kyra van den Akker, Tessa Meursen Marloes van Lochem, 'Aanmeren. Verkenning ondermijning op watergebonden bedrijventerreinen, 2025.

66 Anton van Wijk, Edward van der Torre, Gerine van Barnevelden Joey Wolsink, 'Ondermijning op en rond luchthaven Schiphol', 2020; RIEC Limburg, 'Meerjarenbeleidsplan 2025-2028', 09-2024; Richard Staring, Emily Berger, Juno van Esseveldten Joey Wolsink, 'Eindhoven Airport belicht. Veiligheid, (transit)criminaliteit en de aanpak van ondermijning', 2024; RIEC Oost-Brabant, 'Meerjarenbeleidsplan RIEC Oost-Brabant 2025-2028', 2024.

67 Gorsica Madelijne, 'Geconstrueerd vertrouwen. Een dossieronderzoek naar crimineel misbruik van de trustsector', in WODC Justitiële verkenningen, jrg. 50, nr. 2, 2024, p. 92-105.

68 Platform Veilig Ondernemen, 'De impact van ondermijning op ondernemers', 21-05-2025; RIEC Den Haag, 'Ontwikkelstrategie 2025 tot en met 2028. Één coalitie tegen ondermijning', 2024; RIEC Zeeland West-Brabant, 'Meerjarenbeleidsplan 2025-2028', 2024; Europol, 'Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures', 12-2024.

69 SKC, 'Expertmeeting Financieel', 2025.

70 Europol, 'Decoding the EU's most threatening criminal networks', 2024; Driehoek tegen Drugscriminaliteit, 'Rapportage: Visie en Voortgang', 04-2024; FIOD, 'Dreigingsbeeld Poortwachters. Een overzicht van witwasdreigingen die raken aan de rol van poortwachters', 10-2024; SKC, 'Expertmeeting Advocatuur', 2025.

71 Iris Blatter en Toine Spapens, 'Ondermijning op het platteland. Problemen en aanpak', 20-06-2023; RIEC Amsterdam-Amstelland, 'Souvenirwinkels en criminele geldstromen. Een analyse van aanwijzingen voor ondergronds bankieren en het verplaatsen van (crimineel) vermogen via souvenirwinkels in Amsterdam', 19-12-2023; Gemeente Amsterdam, 'De parallelle economie in de Amsterdamse binnenstad', 10-2024.

72 SKC, 'Expertmeeting Financieel', 2025; 'Expertmeeting Publiek-Privaat', 2025.

73 Wetenschappelijke Raad voor het Regeringsbeleid, 'Aandacht voor media. Naar nieuwe waarborgen voor hun democratische functies', 03-10-2024.

74 Jilian Snider, 'Solving Crime, Protecting Communities: A Blueprint for Safer Streets', 06-2025.

75 Politie, 'Visie op jonge aanwas in de zware criminaliteit vanuit de onderwereld. "Ze willen allemaal Tony Montana zijn"', 03-2023; Jan Meus, 'Narco's in Nederland. Van Brabantse pillenboeren tot internationale cocaïnesmokkelaars', 2024.

76 C.A.J. van den Eeden, R.A. Roks, M.V. van Koppen, J.H. Goes, S.J. van Deuverenen L.K. Krijger, 'Georganiseerde criminaliteit in Nederland: cocaïnesmokkel en liquidaties – Zesde rapportage op basis van de Monitor Georganiseerde Criminaliteit', 2026.

77 SKC, 'Expertmeeting Financieel', 2025; Kruisbergen Edwin en Soudijn Melvin,' Parallelle economie. Over ontwijken van en verzet tegen regulier financieel-economisch verkeer-een introductie, in WODC Justitiële verkenningen, jrg. 50, nr. 2, 2024, p. 19.

78 NOS, 'Aantal uitleveringen stijgt: Dubai geen veilige haven meer voor criminelen', 02-11-2024, https://nos.nl/artikel/2586276-aantal-uitleveringen-stijgt-dubai-geen-veilige-haven-meer-voor-criminelen.

79 AD, 'Opgejaagde criminelen duiken onder in bruisend Marokko', 05-10-2025, www.ad.nl/binnenland/criminelen-vluchten-van-dubai-naar-marokko-per-privejet-of-luxe-container~a478ed27/.

80 Telegraaf, 'Toeristenparadijs Costa del Sol is steeds vaker toneel van dodelijk geweld', 18-10-2025, www.telegraaf.nl/nieuws/mocro-maffia-overspoelt-marbella-met-extreem-geweld-ze-moorden-elkaar-uit-deze-generatie-geeft-nergens-om/97266179.html.

81 Karin van Wingerde, Lieselot Bisschop en Felix Brongers, 'Onbedoeld ondermijnen: Verkennend onderzoek naar de wijze waarop de Nederlandse Overheid onbedoeld de georganiseerde drugscriminaliteit kan faciliteren', 2023.

82 SKC, 'Expertmeeting Bestuurlijk', 2025.

83 Gemeente Amsterdam, 'Position paper Amsterdam, Breda, Den Haag, Rotterdam en Utrecht t.b.v. commissiedebat criminaliteitsbestrijding, ondermijning en georganiseerde criminaliteit van 6 februari 2025', 19-05-2025.

84 SKC, 'Expertmeeting Opsporing en toezicht', 2025; SKC, 'Expertmeeting Financieel', 2025.

85 Taskforce gegevensdeling, 'Special Zomer 2025', 2025.

86 SKC, 'Expertmeeting Publiek-Privaat', 2025.

87 SKC, 'Expertmeeting Opsporing en toezicht', 2025.

88 Hans Nelen, Karin van Wingende, Lieselot Bisschopen Roland Moerland, 'Koers bepalen. Over de lessen van de versterking aanpak georganiseerde drugscriminaliteit', 2023.

89 Taskforce gegevensdeling, 'Special Zomer 2025', 2025

90 Taskforce gegevensdeling, 'Special Zomer 2025', 2025.

91 SKC, 'Expertmeeting Publiek-Privaat', 2025; SKC, 'Expertmeeting Opsporing en toezicht', 2025; 'Expertmeeting Financieel', 2025; SKC, 'Expertmeeting Publiek-privaat', 2025..

92 Follow the Money, 'Meer dan 50 algoritmes van de Belastingdienst zijn illegaal, zegt de Autoriteit Persoonsgegevens', 11-10-2025.

93 Ministerie van Volksgezondheid, Welzijn en Sport, 'Samen de lat hoger leggen: Onderzoek naar de governance en het tuchtrecht voor veilige en integere sport', 2023.

94 Iris Blatter en Toine Spapens, 'Ondermijning op het platteland. Problemen en aanpak', 20-06-2023.

95 Genoemd tijdens diverse expertmeetings.

96 Taskforce Gegevensdeling, "zonder goede gegevensdeling laat je inwoners in de kou staan", Sybrand Buma, 03-12-2025, https://jenvgegevens.pleio.nl/news/view/e99568fc-de39-443d-8b42-4bcf3183c64c/zonder-goede-gegevensdeling-laat-je-inwoners-in-de-kou-staan-sybrand-buma.

97 Schmitz, Michael, 'Trade based money laundering: uitdagingen en ontwikkelingen binnen de opsporing', in Justitiële verkenningen Parallelle economie, jrg. 50, 2024, p. 83.

98 SKC, 'Expertmeeting opsporing en toezicht', 2025; feedback op eerder concept.

99 SKC, 'Expertmeeting Advocatuur', 2025.

100 SKC, 'Expertmeeting Financieel', 2025.

101 RIEC Limburg, 'Fenomeenonderzoek Nieuwe Psychoactieve Stoffen (NPS)', 12-2023.

102 Rijksoverheid, 'Designerdrugsverbod vanaf 1 juli van kracht', 07-2025. www.rijksoverheid.nl/actueel/nieuws/2025/07/01/designerdrugsverbod-vanaf-1-juli-van-kracht.

103 Rijksoverheid, Kabinet gaat synthetische opioïden nitazenen verbieden, 09-2025, www.rijksoverheid.nl/actueel/nieuws/2025/09/26/kabinet-gaat-synthetische-opioiden-nitazenen-verbieden.

104 SKC, 'Expertmeeting opsporing en toezicht', 2025.

105 Trimbos instituut, 'Wees voorzichtig met zeggen dat drugsgebruik normaal is', 14-12-2023 (geraadpleegd 13-04-2026), www.trimbos.nl/actueel/blogs/wees-voorzichtig-met-zeggen-dat-drugsgebruik-normaal-is/.

106 Trimbos instituut, 'Nationale Drug Monitor, editie 2026. Kerncijfers alcohol, tabak en drugs - Nationale Drug Monitor, 17-02-2026 (geraadpleegd op: 13-04-2026), www.nationaledrugmonitor.nl/kerncijfers-alcohol-tabak-en-drugs/.

107 Trimbos instituut, 'Rapport Het Grote Uitgaansonderzoek 2023. Uitgaanspatronen, middelengebruik, gezondheid en intentie tot stoppen of minderen onder uitgaande jongeren en jongvolwassenen', 06-10-2025, p. 5, www.trimbos.nl/kennisbank/rapport-het-grote-uitgaansonderzoek-2023/.

108 SKC, 'Expertmeeting opsporing en toezicht', 2025.

109 SKC, 'Expertmeeting Publiek-privaat', 2025.

110 Bureaubroekhuizen, 'Meldingsbereidheid ondermijnende criminaliteit', 2022; RIVM, 'Themastudie georganiseerde criminaliteit Ondermijning van de democratische rechtstaat en andere verbindingen met de nationale veiligheid', 2021.

111 SCP, 'Sociale en Culturele Ontwikkelingen 2025', 2025; SCP, 'Samenleven in de toekomst: een verkenning naar sociale cohesie bij een veranderde bevolkingssamenstelling 2050', 2024.

112 SCP, 'Sociale en Culturele Ontwikkelingen 2025', 2025; SCP, 'Samenleven in de toekomst: een verkenning naar sociale cohesie bij een veranderde bevolkingssamenstelling 2050', 2024.

113 SCP, 'Sociale en Culturele Ontwikkelingen 2025', 2025; SCP, 'Samenleven in de toekomst: een verkenning naar sociale cohesie bij een veranderde bevolkingssamenstelling 2050', 2024.

114 CBS, 'Vertrouwen in mensen en in organisaties; persoonskenmerken', geraadpleegd op 04-02-2026 via www.cbs.nl/nl-nl/cijfers/detail/85533NED?q=keyword:institutioneel%20vertrouwen.

115 Sociaal en Cultureel Planbureau, 'Sociale en Culturele Ontwikkelingen 2025 (Factsheet)', 18-02-2025, www.scp.nl/site/binaries/site-content/collections/documents/2025/02/18/sociale-en-culturele-ontwikkelingen-2025/scp-factsheet-sociale-en-culturele-ontwikkelingen-2025.pdf.

116 NCTV, 'Soevereinenbeweging ondermijnt democratische rechtsorde', 09-04-2024 (geraadpleegd op 16-02-2026), www.nctv.nl/actueel/nieuws/2024/04/09/soevereinenbeweging-ondermijnt-democratische-rechtsorde.

117 Parool, 'Zo bindt de Zeehavenpolitie de strijd aan met cocaïnebendes en hun handlangers: 'Er komt hier geen partij drugs binnen zonder corruptie', 08-06-2024.

118 Van de AIVD verkregen informatie en met toestemming opgenomen.

119 Ministerie van Justitie en Veiligheid en het Ministerie van Economische Zaken en Klimaat, 'Handreiking voor kwetsbare branches in de strijd tegen georganiseerde, ondermijnende criminaliteit', 2024.

120 Parool, 'Zo bindt de Zeehavenpolitie de strijd aan met cocaïnebendes en hun handlangers: 'Er komt hier geen partij drugs binnen zonder corruptie'', 08-06-2024.

121 Van de AIVD verkregen informatie en met toestemming opgenomen.

122 NCTV, 'Cybersecuritybeeld Nederland 2025. Riskant een mix in een onvoorspelbare wereld', 11-2025.

123 NRC, 'Hackers Odido publiceren alle klantgegevens, 02-03-2026, www.nrc.nl/nieuws/2026/03/01/criminele-hackers-odido-publiceren-alle-klantgegevens-a4921823.

124 Van de AIVD verkregen informatie en met toestemming opgenomen.

125 Ministerie van Justitie en Veiligheid en het Ministerie van Economische Zaken en Klimaat, 'Handreiking voor kwetsbare branches in de strijd tegen georganiseerde, ondermijnende criminaliteit', 2024.

126 Van de AIVD verkregen informatie en met toestemming opgenomen.

127 NCTV, 'Cybersecuritybeeld Nederland 2024', 2024.

128 NRC, 'Locatiedata van EU-functionarissen verkrijgbaar. Is dat wel legaal?', 2025.

129 SKC, 'Expertmeeting Opsporing en Toezicht', 2025.

130 De Volkskrant. 'Drieënhalf jaar cel geëist tegen lekkende politieman: 'Als ik niet meewerkte, zouden ze mijn kinderen ontvoeren'. ', 24-06-2025; NOS Nieuws, 'Celstraf voor ex-politieagent voor lekken informatie op verzoek van broer', 8-7-2025.

131 Europol,' Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures', 12-2024.

132 Politie Midden-Nederland, 'Ondermijning in de zorg: een grote zorg', 2024; Politie, 'Fenomeenbeeld 2024: Online fraude in beeld', 2024.

133 Anton van Wijk, Edward van der Torre, Gerine van Barnevelden Joey Wolsink, 'Ondermijning op en rond luchthaven Schiphol',

2020; Richard Staring, Emily Berger, Juno van Esseveldten Joey Wolsink, 'Eindhoven Airport Belicht. Veiligheid (transit)criminaliteit en de aanpak van ondermijning', 2024; Liz van Blitterswijk en Marlou Brokx, 'Rapportage: Ondermijning in het sierteelttransport. Een actiegericht onderzoek in opdracht van het RIEC Den Haag en de Aanpak Weerbare Sierteeltsector', 18-03-2025; RIEC Zeeland West-Brabant, 'Fenomeenbeeld Binwnenvaart Noord-Brabant en Zeeland. Thema: cocaïne', 21-08-2025; Taskforce – RIEC Brabant – Zeeland, 'EHHK Price', 02-2024; RIEC Den Haag, 'Ondermijning in het buitengebied en de (glas)tuinbouw', 03-2022.

134 Presentatie van toezichthoudende partij aan SKC.

135 SKC, 'Achtergrondgesprek met Sociaal Cultureel Planbureau', 12-01-2016.

136 FIOD, 'Corruptie', 2021, www.fiod.nl/opsporingsthemas/corruptie/. Geraadpleegd op 06-04-2024); Transparency International, 'What is corruption?', 2024, www.transparency.org/en/what-is-corruption (geraadpleegd op 06-04-2024).

137 Zürcher, E., Pardal, M., Leussink, I.en Stijn, E. (2024). 'Drugsgerelateerde corruptie op Schiphol en in de Rotterdamse haven: Een analyse van corruptiedreigingen, impact en beleidsinstrumenten op basis van de methodologie voor National Risk Assessment' In RAND Corporation eBooks, 2024,p.6. https://doi.org/10.7249/rra2870-1.

138 Winter, H., Woestenburg, N., Struiksma, N., Akerboom, C., Boxum, C.en Smits, J. 'Criminele beïnvloeding van het lokale openbaar bestuur' Rijksuniversiteit Groningen / Pro Facto, 2017, p. 15. https://repository.wodc.nl/handle/20.500.12832/2284.

139 Savona, E. U.en Berlusconi, G. (Red),'Organised Crime Infiltration of Legitimate Businesses in Europe: A Pilot Project in Five European Countries. Transcrime', 2015 p. 19, www.transcrime.it/wp-content/uploads/2015/11/Project-ARIEL_Final-report.pdf.

140 Europol, 'The changing DNA of serious and organised crime', 2025.

141 Brabants Dagblad, 'Hoe criminelen hun klauwen in tiener Mike slaan' 16-08-2025.

142 SKC, 'Expertmeeting Financieel', 2025.

143 SKC, 'Expertmeeting Bestuurlijk', 2025.

144 Het Parool, 'In Drie jaar van 100 naar 70.000 Oekraïense dronepiloten: dit is de oorlog van de drones geworden', 2025

145 Paddy Ginn en Alex Goodwin, 'Crime by drone: A new paradigm for organised crime', 2025.

146 Phil Williams, 'The Fifth Wave: Organizes crime in 2040', 2024; Europol, 'The Unmanned Future9S0. The impact of robotics and unmanned systems on law enforcement', 2025.

147 The Guardian, 'Colombia identifies new threat in drug war: the autonomous narco drone sub', 2025.

148 Rijnmond, 'Drone met hasj en telefoon haalt de gevangenis niet, dronepiloot gepakt', 06-02-2026, www.rijnmond.nl/nieuws/2148571/drone-met-hasj-en-telefoon-haalt-de-gevangenis-niet-dronepiloot-gepakt.

149 De Telegraaf, 'Ontsnapping 2.0: Tillen drones gedetineerden straks over de gevangenismuur? Engelse gevangenisinspecteur waarschuwt', 2025.

150 De Gazet van Antwerpen, 'Ook Antwerps burgemeester Els van Doesburg was mogelijk doelwit van terreurverdachten', 2025.

151 Vereniging Innovatie Geneesmiddelen, 'AI bij ontwikkeling geneesmiddelen: kansen en keuze', 12-06-2025, www.vereniginginnovatievegeneesmiddelen.nl/kennisbank/ai-bij-ontwikkeling-geneesmiddelen-kansen-en-keuzes/

152 RDI, 'Toepassingen van AI', www.rdi.nl/onderwerpen/technologische-ontwikkelingen/kunstmatige-intelligentie/toepassingen-van-kunstmatige-intelligentie-ai.

153 Tang, X., Dai, H., Knight, E., Wu, F., Li, Y., Li, T.en Gerstein, M., 'A survey of generative AI for de novo drug design: new frontiers in molecule and protein generation. Briefings in Bioinformatics, 25(4), 07-2024.

154 Reuters, 'Europol warns AI driven crime threats, 18-03-2025, www.reuters.com/world/europe/europol-warns-ai-driven-crime-threats-2025-03-18.

155 Algemeen Dagblad, 'Waarom gameplatform Roblox wereldwijd onder vuur ligt: 'Veel ouders hebben geen idee', 11-01-2026, www.ad.nl/tech/waarom-gameplatform-roblox-wereldwijd-onder-vuur-ligt-veel-ouders-hebben-geen-idee~a677b817/.

156 Phil Williams, 'The Fifth Wave: Organised crime in 2040', 2024.

157 Koen Aartsma, Liam Kleinen Chiara Schrader, 'Clingendael strategische monitor 2025-2030: Geopolitiek changement op het wereldtoneel', 01-2025.

158 NCTV, 'Hoofdrapport Trendanalyse Nationale Veiligheid 2024', 2024.

159 Ducheine, P. A. L., Pijpers, P. B. M. J.en Arnold, K. L. 'The 'next' war should have been fought in cyberspace, right? An analysis of cyber-activities in the 2022 Russo-Ukraine war, 2022, p. 6-8.

160 UNODC, 'As war rages on in Ukraine, organised crime is taking new forms', United Nations Office at Geneva, 2025, www.ungeneva.org/en/news-media/news/2025/07/108615/as-war-rages-ukraine-organised-crime-taking-new-forms.

161 Koen Aartsma, Liam Kleinen Chiara Schrader, 'Clingendael strategische monitor 2025-2030: Geopolitiek changement op het wereldtoneel', 01-2025.

162 Politie, 'Online Fraude in Beeld. Fenomeenbeeld 2024', 2024; RIEC Amsterdam-Amstelland, 'Kennisdocument Cryptobetaalkaarten en criminele geldstromen', 2024.

163 SKC, 'Groepsinterview Stable Coins', 2025.

164 Openbaar Ministerie, 'Jaaroverzicht Criminele Geldstromen 2024', 2024; National Crime Agency, 'National Strategic Assessment 2025 of Serious and Organised Crime', 2025; SKC, 'Groepsinterview Stable Coins', 2025.

165 RTL, 'Tiener werd geronseld om te schieten op huis Alphen aan den Rijn: 'Wilde snel geld verdienen'', 18-09-2025; Leidsch Dagblad, ''Finfluencer te rooskleurig': onderzoek Jongeren willen snel veel geld verdienen', 16-03-2024.

166 Vakblad Fondsenwerving, ''Survival of the Richest': ongelijkheid groeit steeds verder', 16-01-2023.

167 SKC, 'Achtergrondgesprek met Sociaal Cultureel Planbureau', 12-01-2016; CE Noticias Financieras English, 'individualism and loneliness, the combination that defines a paradox of modern life', 11-14-2025.

168 SKC, 'Achtergrondgesprek met Sociaal Cultureel Planbureau', 12-01-2016.

169 Mondiale opgaven voor inclusieve groene groei, 'Notitie ten behoeve van de directie Inclusieve Groene Groei', Buitenlandse Handel en Ontwikkelingssamenwerking', 20-06-2018.

170 Financial Times, 'Droughts are major threat to Eurozone economy, warns ECB', 22-05-2025.

171 WHO, 'What are health consequences of air pollution on populations?', 25-06-2024, www.who.int/news/item/25-06-2024-what-are-health-consequences-of-air-pollution-on-populations?; UN, 'Climate crisis 'affecting quality of life and fuelling discontent', 16-01-2020.

172 The Hague Centre for Strategic Studies, 'Next Generation Organised Crime. Systemic change and the evolving character of modern transnational organised crime', 05-2023.

173 NOS Nieuws, 'Zorgen over criminelen die geld witwassen via bouw, pakketdiensten en zorg', 28-06-2024, https://nos.nl/artikel/2526430-zorgen-over-criminelen-die-geld-witwassen-via-bouw-pakketdiensten-en-zorg.

174 KNB, NVB, NBA, NVM, NRVT, Politie, Vastgoed Ned., Stichting Fraudebestrijding Hypotheken, ZNSTD, KVK, 'Kamerbrief aanpak hypotheekfraude', 17-12-2025; CCV, 'Verschijningsvormen', 28-08-2025, https://hetccv.nl/themas/georganiseerde-criminaliteit-en-ondermijning/vastgoedcriminaliteit/verschijningsvormen-vastgoedcriminaliteit/.

175 Andersson Elffers Felix, 'De parallelle economie in de Amsterdamse binnenstad', 2024.

176 Andersson Elffers Felix, 'De parallelle economie in de Amsterdamse binnenstad', 2024.

177 Brabants Dagblad, 'De verborgen wereld achter een autohandel in Best: drugsmiljoenen witwassen op volle toeren', 06-12-2025, www.bd.nl/eindhoven/de-verborgen-wereld-achter-een-autohandel-in-best-drugsmiljoenen-witwassen-op-volle-toeren~aa7ffeod/; Eindhovens Dagblad, 'Hij zat al in de cel maar Chris S. (53) uit Eindhoven krijgt er jaren bij voor witwassen van drugsgeld via autozaak', 24-02-2026, www.ed.nl/112-nieuws-eindhoven/hij-zat-al-in-de-cel-maar-chris-s-53-uit-eindhoven-krijgt-er-jaren-bij-voor-witwassen-van-drugsgeld-via-autozaak~a848da2f/.

178 Andersson Elffers Felix, 'De parallelle economie in de Amsterdamse binnenstad', 2024.

179 Openbaar Ministerie, 'OM legt Louis Vuitton strafbeschikking op van 500.000 euro', 12-02-2026, www.om.nl/actueel/nieuws/2026/02/12/om-legt-louis-vuitton-strafbeschikking-op-van-500.000-euro..

180 Parool, 'Zo bindt de Zeehavenpolitie de strijd aan met cocaïnebendes en hun handlangers: 'Er komt hier geen partij drugs binnen zonder corruptie', 08-06-2024.

181 Pieter Tops, Edward van der Torre, 'Ondermijning. Over de praktische betekenis van een analytisch begrip', 2024.

182 Staring, R., Bisschop, L., Roks, R., Brein, E. en van de Bunt, H., 'Eindrapport drugscriminaliteit in de Rotterdamse haven', 26-05-2019, www.repub.eur.nl/pub/116670#:~:text=In%20het%20rapport%20"Drugscriminaliteit%20in%20de%20Rotterdamse%20haven%3A,de%20drugssmokkel%20in%20de%20grootste%20haven%20van%20Europa.

183 LIEC, 'Landelijk beeld van ondermijnende criminaliteit', 21-10-2019, www.riec.nl/site/binaries/site-content/collections/documents/2019/10/21/landelijk-beeld/Landelijk+beeld+-def.+verzending+Minister+20191003.pdf

184 Pieter Tops en Edward van der Torre, 'Ondermijning. Over de praktische betekenis van een analytisch begrip', 2024.

185 RIEC Oost-Nederland, Criminele investeringen in vakantieparken in Oost-Nederland: een fenomeenonderzoek, 2022, https://hetccv.nl/app/uploads/2023/09/Rapportage_Vakantieparken_RIECON_i.pdf.

186 Europol, 'Decoding the EU's most threatening criminal networks', 11-10-2024.

187 Investico en De Groene Amsterdammer, 'Betonrot in de rechtsstaat. Helft van de rechters en officieren van justitie bedreigd', 30-10-2023, www.platform-investico.nl/onderzoeken/helft-van-de-rechters-en-officieren-van-justitie-bedreigd

188 HP De Tijd, 'Saskia Belleman en John van den Heuvel: Er moeten grenzen gesteld worden', 17-07-2025.

189 Rechtspraak.nl, 'ECLI:NL:RBOVE:2025:1464', 18-03-2025; Rechtspraak.nl, 'ECLI:NL:RBOVE:2025:1465, 18-03-2025

190 Sociaal Cultureel Planbureau, 'Sociale cohesie in wetenschap en beleid', www.scp.nl/dossiers/sociale-cohesie/sociale-cohesie-in-wetenschap-en-beleid, geraadpleegd op 03-12-2025.

191 Sociaal Cultureel Planbureau, 'Sociale cohesie in wetenschap en beleid', www.scp.nl/dossiers/sociale-cohesie/sociale-cohesie-in-wetenschap-en-beleid, geraadpleegd op 03-12-2025.

192 Pieter Tops en Edward van der Torre, 'Ondermijning. Over de praktische betekenis van een analytisch begrip', 2024, p. 53.

193 EenVandaag, 'Amsterdam en Rotterdam slaan alarm: 'Kwetsbare wijken worden vergiftigd door criminaliteit'', 10-08-2023.

194 Brabants Dagblad, 'Gemeente ziet problemen Kruisstraat telkens weer opduiken en wil het grootser aanpakken', 17-09-2025, www.bd.nl/eindhoven/gemeente-ziet-problemen-kruisstraat-telkens-weer-opduiken-en-wil-het-grootser-aanpakken~a1375496/.

195 Ministeries van Volksgezondheid, Cultuur en Sport & Onderwijs, Cultuur en Wetenschap, 'Rode dradenanalyse criminele inmenging in de amateursport, Een kennisoverzicht van de aard, omvang, risico's en handelingsperspectieven', 2022; Ministerie van Volksgezondheid, Welzijn en Sport, 'Samen de lat hoger leggen: Onderzoek naar de governance en het tuchtrecht voor veilige en integere sport, 02-2023.

196 Ministeries van Volksgezondheid, Cultuur en Sport & Onderwijs, Cultuur en Wetenschap, 'Rode dradenanalyse criminele inmenging in de amateursport, Een kennisoverzicht van de aard, omvang, risico's en handelingsperspectieven', 2022

197 Monique Bruinsma, Vidar Stevens, Rens Cremers en Toine Spapens, Criminele inmenging bij amateursportverenigingen: Aard, omvang en handelingsperspectief, 2020, www.kennisbanksportenbewegen.nl/?file=10166&m=1607499327&action=file.download.

198 Ministeries van Volksgezondheid, Cultuur en Sport & Onderwijs, Cultuur en Wetenschap, 'Rode dradenanalyse criminele inmenging in de amateursport, Een kennisoverzicht van de aard, omvang, risico's en handelingsperspectieven', 2022

199 Politie, Geweld van de georganiseerde misdaad in beeld Fenomeenbeeld 2024, 2024, www.politie.nl/binaries/content/assets/politie/onderwerpen/publicaties/2024/8c001d24-810c-4778-8bc2-e723fdc2ad40.pdf.

200 Monique Bruinsma, Vidar Stevens, Rens Cremers en Toine Spapens, Criminele inmenging bij amateursportverenigingen: Aard, omvang en handelingsperspectief, 2020, www.kennisbank-sportenbewegen.nl/?file=10166&m=1607499327&action=file.download.

201 Teun Voeten, 'Drugs: Antwerpen in de greep van Nederlandse syndicaten', 3e druk, 2020, p.227-228.

202 RTL Nieuws, 'Duizenden huizen in handen van hypotheekfraudeurs, politie slaat alarm', 27-05-2025, www.rtl.nl/nieuws/artikel/5511059/politie-wil-hypotheekfraude-beter-aanpakken; Het Financieele Dagblad, 'Crimineel netwerk kocht honderden woningen via listige hypotheekfraude', 14-07-2024, https://fd.nl/samenleving/1522875/crimineel-netwerk-kocht-honderden-woningen-via-listige-hypotheekfraude.

203 Arjen Koppen, Anja P.G. Wijnands-Kleukers, Femke M.J. Gresnigt en Dylan W. de Lange, 'Clinical toxicology of exposures to chemicals from clandestine drug labouratories: a literature review', 22-02-2025.

204 Strategische Milieukamer, 'Dreigingsbeeld Milieucriminaliteit 2021, 22-07-2021, https://www.om.nl/site/binaries/site-content/collections/documents/milieucriminaliteit/2021/07/index/Dreigingsbeeld+milieucriminaliteit+2021.pdf

205 Strategische Milieukamer, 'Dreigingsbeeld Milieucriminaliteit 2021, 22-07-2021, https://www.om.nl/site/binaries/site-content/collections/documents/milieucriminaliteit/2021/07/index/Dreigingsbeeld+milieucriminaliteit+2021.pdf.

206 De Volkskrant, 'Recordaantal drugslabs in 2024 ontmanteld, vooral in woonwijken', 09-05-2025.

207 NOS,'Drugsafval vermengd met mest uitgereden op Brabantse akkers', 29-08-2024.

208 Politie, 'Samenwerken en uitbesteden: georganiseerde misdaad in beeld. Fenomeenbeelden 2024', 09-2024.

209 Europol, 'Decoding the EU's most threatening criminal networks', 11-10-2024, www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks#downloads.

210 Politie, 'Samenwerken en uitbesteden: georganiseerde misdaad in beeld. Fenomeenbeelden 2024', 09-2024.

211 FIOD, 'Witwassen', 27-10-2021 (update 29-10-2025) (geraadpleegd op 27-02-2026), www.fiod.nl/opsporingsthemas/witwassen/.

212 Wetenschappelijk Onderzoek- en Datacentrum, 'National Risk Assessment Witwassen 2023', 03-04-2024.

213 Financial Intelligence Unit – Nederland, 'Jaaroverzicht FIU-Nederland 2024', 2025, www.fiu-nederland.nl/wp-content/uploads/2025/07/FIU-NL-jaaroverzicht-2024.pdf.

214 European Monitoring Centre for Drugs and Drug Addiction and Europol, 'EU Drug Markets Analysis: Key insights for policy and practice, Publications Office of the European Union, 2024, www.europol.europa.eu/cms/sites/default/files/documents/EU%20Drug%20Markets%20Analysis%202024.pdf.

215 UNODC and EUROPOL, 'The illicit trade of cocaine from Latin America to Europe – from oligopolies to free for-all?', Cocaine Insights 1,September 2021, www.unodc.org/documents/data-and-analysis/cocaine/Cocaine_Insights_2021.pdf.

216 UNODC, 'Global report on Cocaine 2023 – Local dynamics, global challenges', 2023, www.unodc.org/documents/data-and-analysis/cocaine/Global_cocaine_report_2023.pdf.

217 United States Department of State Bureau for International Narcotics and Law Enforcement Affairs, 'International Narcotics Control Strategy Report. Volume 1: Drug and Chemical Control', 03-2025.

218 Sénat.fr, 'Audition de M. Bruno Le Maire, ministre de l'économie, des finances et de la souveraineté industrielle et numérique', 26-03-2024, www.senat.fr/compte-rendu-commissions/20240325/ce_narco.html.

219 Bart De Wever, 'Drugsgeweld komt overgewaaid uit Nederland', De Morgen, 04-04-2018.

220 Bart De Wever 'Ik zie veel motivatie in strijd tegen drugsgeweld' - YouTube (18:11), 17-01-2024.

221 Sjoerd Hooijmaaijers en Sander IJmker, 'De illegale economie en nationaal inkomen', in Justitiële verkenningen Parallelle economie, 50, 2024, p. 30-43.

222 Vrij naar Nederlandse School voor Openbaar Bestuur, 'Ondermijning ondermijnt. Hoe het Rijk meer ruimte kan maken voor een (boven)lokale aanpak van georganiseerde ondermijnende criminaliteit', 2016, p. 8.

223 Bureaubroekhuizen, 'Meldingsbereidheid ondermijnende criminaliteit', 2022; RIVM, 'Themastudie georganiseerde criminaliteit Ondermijning van de democratische rechtstaat en andere verbindingen met de nationale veiligheid', 2021.

224 RIEC Amsterdam-Amstelland, 'Meerjarenplan 2025-2028', 09-2024.

225 Analistennetwerk Nationale Veiligheid, 'Themastudie georganiseerde criminaliteit. Ondermijning van de democratische rechtsstaat en andere verbindingen met de nationale veiligheid', 01-2021.

226 Analistennetwerk Nationale Veiligheid, 'Leidraad risicobeoordeling Rijksbrede Risicoanalyse Nationale Veiligheid', 07-2022.

227 'Koester de democratie! Een dringende oproep om de democratische rechtsorde weer voor iedereén te laten werken.', 02-11-2023 p. 7.

228 RTL Nieuws, 'Duizenden huizen in handen van hypotheekfraudeurs, politie slaat alarm', 27-05-2025, www.rtl.nl/nieuws/artikel/5511059/politie-wil-hypotheekfraude-beter-aanpakken.

229 SKC, 'Expertmeeting Financieel', 2025.

230 Trouw, 'Criminelen willen horecabazen 'helpen' bij hun geldnood na de overstroming in Zuid-Limburg', 28-08-2023.

231 Trimbos-instituut, 'Legaal, maar niet bereikbaar: medicinale cannabis in Nederland', 02-02-2026, www.trimbos.nl/actueel/nieuws/legaal-maar-niet-bereikbaar-medicinale-cannabis-in-nederland/.

232 C.A.J. van den Eeden, R.A. Roks, M.V. van Koppen, J.H. Goes, S.J. van Deuveren en L.K. Krijger, 'Georganiseerde criminaliteit in Nederland: cocaïnesmokkel en liquidaties – Zesde rapportage op basis van de Monitor Georganiseerde Criminaliteit', 2026.

233 SKC, 'Themastudie Jeugd: Hoe jongeren als pionnen worden bewogen in het schaakspel van de georganiseerde criminaliteit', 2026; Politie, 'Praat erover: start campagne tegen online benaderen van jongeren voor criminele klusjes', 20-11-2025.

234 Financial Intelligence Unit – Nederland, 'Jaaroverzicht FIU-Nederland 2024', 2024.

235 BijzonderStrafrecht, 'Katvanger faciliteert omvangrijkse PGB-fraude en wordt veroordeeld voor oplichting en gewoontewitwassen', 02-07-2025; BijzonderStrafrecht, 'Veroordeling wegens voorbereiding verkoop staatsgeheimen', 26-04-2013; AD, 'Monteurs verdacht van uithaalklussen in de haven: 'Zeer zwaar georganiseerde criminaliteit'', 24-10-2024.

236 FIU, 'Jaaroverzicht 2024: Bedrijven misbruikt als dekmantel', 02-07-2025.

237 RIEC Limburg, 'Ondermijnende criminaliteit in Limburg', 09-2020.

238 NOS, 'Derde advocaat van Taghi opgepakt op verdenking van deelname aan criminele organisatie.' 10-04-2025; NOS, 'Overige twee advocaten Taghi leggen verdediging neer'. 16-04-2025; NOS, 'Hof neemt vier maanden extra voor zoektocht naar advocaat Taghi'. 06-11-2025.

239 SKC, 'Expertmeeting Advocatuur', 2025.

240 FIU-Nederland, 'Jaaroverzicht 2024', 06-2025.

241 Europol, 'Leveraging legitimacy: How the EU's most threatening criminal networks abuse legal business structures', 12-2024; FIU-Nederland, 'Jaaroverzicht 2024', 06-2025.

242 Omroep Zeeland, 'Bulk Terminal Zeeland: in tien jaar tijd tien keer zo groot, in drie maanden failliet', 07-08-2025; PZC.nl, 'De zaak Bulk Terminal Zeeland: over big bags met een roze lintje en tien procent van de waarde van de cocaïne', 8-8-2024; PZC.nl, 'Witte rook in Zeeuwse drugszaak: na lange vertraging begint in juni proces BTZ-directie', 1-12-2025; PZC.nl, 'Voorfinale Bulk Terminal Zeeland: Ko de K. grijpt laatste kans aan om onschuld te bewijzen vlak voor de definitieve ontknoping', 26-03-2026.

243 Anti-Financial Crime & Financial Crime Compliance, 'INSIGHT: How Europe's organised crime networks use construction, hospitality and logistics sectors to launder dirty money', 05-04-2024; European Union Agency for Criminal Justice Coorperation, 'Drug trafficking network active across Europe dismantled', 02-07-2024.

244 Europol, 'European Union Serious and Organised Crime Threat Assessment. The changing DNA of serious and organised crime', 2025.

245 Marco Di Cataldo, Nicola Mastrorocco. 'Organised Crime, Captured Politicians, and the Allocation of Public Resources' The Journal of Law, Economics, and Organisation, Volume 38, Issue 3, 11-2022, p 813.

246 NOS.nl, 'Yesilgöz na dreigberichten over Amalia: georganiseerde misdaad fundamenteel probleem', 18-09-2022; DutchNews.nl, 'Security stepped up for princess Amalia and Mark Rutte after underworld 'threats', 19-09-2022; Volkskrant, 'Waarom moet Amalia binnenblijven, ondanks haar zware beveiliging?', 14-10-2022.

247 Trouw, Poging tot ontvoering minister: het drugsgeweld in België beperkt zich niet langer tot de onderwereld, 25-09-2022; Volkskrant, 'Verdachten van ontvoeringsplannen voor Belgische justitieminister worden overgeleverd aan België, 26-10-2022.

248 Julien van Ostaaijen en Meijze Sweere (e.a.), 'Een kwetsbaar ambt. Over ondermijning en oneigenlijke druk op decentrale volksvertegenwoordigers', 09-2024, https://open.overheid.nl/documenten/9681e06a-4e4f-42f8-94cf-6a18cd12e64e/file.

249 NOS, 'OM bestempelt moord op De Vries als terrorisme, verdediging bestrijdt dit', 13-10-2022; NOS,'OM eist in hoger beroep levenslang voor liquidatie Peter R. de Vries', 09-10-2025.

250 AD, ''Bolle Jos' heet soms ook Jacob, Willem, Ernst, Edin of Omar', 03-05-2025.

251 WNL,'Is misdaadjournalistiek gevaarlijker geworden? 'Je loopt echt wel kans om doodgeschoten te worden', zegt Marian Husken', 22-05-2025, https://wnl.tv/2025/05/22/misdaadjournalisten-worstelen-met-ernstige-bedreigingen-je-loopt-echt-wel-kans-om-doodgeschoten-te-worden; BNNVARA, 'Misdaadjournalist Paul Vugts: 'Als ik buiten was, was ik nooit meer alleen. Altijd met een ploeg beveiligers.' Wat is het waard?', 26-05-2024, www.bnnvara.nl/artikelen/misdaadjournalist-paul-vugts-als-ik-buiten-was-was-ik-nooit-meer-alleen-altijd-met-een-ploeg-beveiligers-wat-is-het-waard; HP De Tijd, 'Saskia Belleman en John van den Heuvel: Er moeten grenzen gesteld worden', 17-07-2025.

252 AIVD, '2024. AIVD jaarverslag, 24-04-2025, p 15-17, www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2025/04/24/jaarverslag-2024/AIVD+Jaarverslag+2024+.pdf.

253 Onderzoeksraad voor Veiligheid, 'Bewaken en beveiligen. Lessen uit drie beveiligingssituaties', 02-2023, p. 6, 12-13.

254 OM, 'Medewerkster rechtbank aangehouden voor schending geheimhoudingsplicht', 13-03-2025, www.om.nl/actueel/nieuws/2025/03/13/medewerkster-rechtbank-aanhouden-voor-schending-geheimhoudingsplicht.

255 RTL Nieuws, Criminelen infiltreren gemeentehuis tientallen keren per jaar, 01-12-2023, www.rtl.nl/nieuws/artikel/5415295/criminelen-infiltreren-gemeentehuis-tientallen-keren-jaar.

256 AIVD, '2024. AIVD jaarverslag, 24-04-2025, p 15-17, www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2025/04/24/jaarverslag-2024/AIVD+Jaarverslag+2024+.pdf.

257 AIVD, '2024. AIVD jaarverslag, 24-04-2025, p 15-17, www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2025/04/24/jaarverslag-2024/AIVD+Jaarverslag+2024+.pdf.

258 Politie, Samenwerken en uitbesteden: georganiseerde misdaad in beeld. Fenomeenbeelden 2024', 09-2024, p. 68, www.politie.nl/binaries/content/assets/politie/onderwerpen/publicaties/2024/317712e8-1458-4b4c-bb2c-740f53089391.pdf.

259 RTL, 'Dode man die aan verkeersbord Brussel hing, zou Albanese drugssmokelaar zijn', 03-10-2025.

260 Mehlbaum, S., J. Broekhuizen en K. van den Akker, 'Ongekend. Een onderzoek naar de impact van dreiging vanuit

de georganiseerde criminaliteit op politiewerk', Politie en Wetenschap, 14-06-2024, www.politieenwetenschap.nl/download/?i=7dff3237e36621d2b207d7ca559efc5e0b6b7437e-303aa7a&p=09d57b72f7eac0d2bd88134e479dbd87e10f-f3876d5965b8.

261 Het Parool, 'Jonge Nederlandse criminelen plegen grof geweld op bestelling in heel Europa – en de opdrachtgever kijkt live mee', 25-10-2025, www.parool.nl/misdaad/jonge-nederlandse-criminelen-plegen-grof-geweld-op-bestelling-in-heel-europa-en-de-opdrachtgever-kijkt-live-mee~b532afd6/.

262 Liebregts, N., Meijer, R., Wesseling, M. en Van den Eeden, C. A. J., 'Ondergronds bankieren in relatie tot georganiseerde criminaliteit in Nederland. Nieuw fenomeen of oud systeem?', 2025.

263 Feedback op eerdere conceptversie van organisatie met kennis van zaken hierover.

264 Feedback op eerdere conceptversie van organisatie met kennis van zaken hierover.

265 KPMG Advisory N.V., 'Krachten gebundeld: naar een effectievere en efficiëntere invulling van de poortwachtersrol in Nederland' 08-2023, p 6, 17, 28, https://assets.kpmg.com/content/dam/kpmg/nl/pdf/2025/sectoren/krachten-gebundeld-markets.pdf.; SKC, 'Expertmeeting financieel', 2025; van Meijgaard, L. 'Position Paper ECTF t.b.v. rondetafegesprek Online fraude d.d. 01-10-2025', www.tweedekamer.nl/downloads/document?id=2025D40350.

266 '#24-JeroenPoelert & RobindeJager over Crimineel Ondergronds Bankieren. Podcast #ondermijning', 14-05-2025.

267 Verburgh Thijmen, Rijs, Jocelyn van, 'De vermenging van ideologie en criminaliteit bij cryptovaluta', in WODC Justitiële verkenningen, jrg. 50, nr. 2, 2024, p. 106-120.

268 AFM, 'Crypto's grotendeels buiten toezicht AFM', www.afm.nl/nl-nl/consumenten/themas/crypto/buiten-toezicht-afm

269 SKC, 'Gespreksverslag (stable) coins', 11-11-2025.

270 NOS, 'Penthouse in Veghel gaat voor miljoen euro aan bitcoins van de hand', 30-04-2021.

271 N. Liebregts R. Meijer M. Wesseling C.A.J. van den Eeden. 'Ondergronds bankieren in relatie tot georganiseerde criminaliteit in Nederland' WODC, 2025, p13.

272 NOS, 'Jpegje van 57 miljoen: recordbedrag voor digitaal kunstwerk', 11-03-2021.

273 The New York Times, 'The Crypto Industry's $28 Billion in 'Dirty Money'', 17-11-2025.

274 De Telegraaf, 'Lopen tegen grenzen aan'; Georganiseerde misdaad steeds slimmer in wegsluizen geld, Openbaar Ministerie vist achter het net', 15-04-2025. Zie wat betreft bedragen ook: Openbaar Ministerie, 'Jaaroverzicht criminele geldstromen 2024, 06-2025'.

275 NCTV, 'Cybersecuritybeeld Nederland 2024', 2024.

276 AIVD, MIVD, NCTV, 'Dreigingsbeeld Statelijke Actoren 2025. Aanhoudende dreigingen in tijden van groeiende onzekerheid', 07-2025.

277 NCTV, 'Cybersecuritybeeld Nederland 2025. Riskant een mix in een onvoorspelbare wereld', 11-2025.

278 Strategisch Kenniscentrum Ondermijnende Criminaliteit, 'Afrika: Transnationaal Ondermijningsbeeld', 2025, https://indd.adobe.com/view/203c4df0-742e-4218-82f6-ce352aa9916f.

279 Europol, 'EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2025', 2025.

280 Brigitte Slot, Niels van Wanrooij, Monique Bruinsmaen Saraï Sapulete, 'Verwevenheid georganiseerde misdaad en terrorisme bij verwerving van vuurwapens', 2017.

281 Frank Renout en Cyril Rosman, 'Drie Nederlanders gehoord over aanslag Bataclan, ze zouden meer weten over wapendeals', 08-03-2022.

282 European Parlementairy Research Service, 'Understanding EU policy on firearms trafficking', 10-2024, www.europarl.europa.eu/RegData/etudes/BRIE/2024/762476/EPRS_BRI(2024)762476_EN.pdf.

283 Europol, 'EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2025', 2025.

284 Signpost Six, 'Insider Risk Trend Report 2026', 02-2026.

285 AIVD, '2024. AIVD jaarverslag, 24-04-2025, p 15-17, www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2025/04/24/jaarverslag-2024/AIVD+Jaarverslag+2024+.pdf.

286 AIVD, MIVD, NCTV, 'Dreigingsbeeld Statelijke Actoren 2025. Aanhoudende dreigingen in tijden van groeiende onzekerheid', 07-2025.

287 NOS.nl, 'Van advocaat tot wapenhandelaar: aangehouden soevereinen vormen gemengde groep', 12-06-2025, https://nos.nl/artikel/2570909-van-advocaat-tot-wapenhandelaar-aangehouden-soevereinen-vormen-gemengde-groep.

288 NCTV, 'Dreigingsbeeld Terrorisme Nederland 2025', 09-12-2025.

289 NCTV, 'Cybersecuritybeeld Nederland 2025. Riskant een mix in een onvoorspelbare wereld', 11-2025.

290 AIVD, MIVD, NCTV, 'Dreigingsbeeld Statelijke Actoren 2025. Aanhoudende dreigingen in tijden van groeiende onzekerheid', 07-2025.

291 AIVD, '2024. AIVD jaarverslag, 24-04-2025.

292 Ministerie van Defensie, 'Openbaar jaarverslag 2024 Militaire inlichtingen-en Veiligheidsdienst, 22-04-2025.

Disclaimer

This is a publication of:

Strategic Knowledge Centre Subversive Crime

www.skc-oc.nl

June 2026 | Subversion Threat Assessment Netherlands (STAN)