


# CROSS-AGENCY SITUATION REPORT 2025



Swedish Coast Guard  
Swedish Customs  
Swedish Economic Crime Authority  
Swedish Enforcement Authority  
Swedish Migration Agency  
Swedish Payments Agency  
Swedish Pensions Agency  
Swedish Police Authority  
Swedish Prison and Probation Service  
Swedish Prosecution Authority  
Swedish Public Employment Service  
Swedish Security Service  
Swedish Social Insurance Agency  
Swedish Tax Agency



**Publisher:** Swedish Police Authority, National Operations Department, 106 75 Stockholm

**Date:** 12.12.2025

**Ref no:** A022.594/2024

**Serial no:** 492

**Graphic design:** Spoon

**Photos:** Midjourney AI pages 1, 21 and 32. Unsplash pages 2, 5, 7, 23, 25 and 31. Swedish Police Authority page 29.

**Printed by:** Swedish Police Authority printing works, Stockholm, December 2025



# Contents

<b>Contents</b>	<b>3</b>
<b>Summary</b>	<b>4</b>
Organised crime is a broad and complex problem	4
The most serious threats affect society's critical assets	4
Organised crime networks exploit society's vulnerabilities	5
Organised crime networks are flexible and adaptable	5
<b>Introduction</b>	<b>6</b>
The cross-agency initiative	6
About the report	6
The structure of the report	6
<b>Organised crime is a broad and complex problem</b>	<b>8</b>
Crime infrastructure	9
Coherent crime strategy	10
Criminal finances and money laundering	12
<b>Crime areas</b>	<b>13</b>
<b>Crime categories with elements of all types of crime infrastructure</b>	<b>13</b>
Drug-related crime	13
Environmental crime	14
Fraud	15
Organised theft	16
Sanctions evasion	17
<b>Crime categories with elements of five types of crime infrastructure</b>	<b>17</b>
Excise fraud	17
Organised crime in working life	18
VAT fraud	19
<b>Crime categories with elements of four types of criminal infrastructure</b>	<b>20</b>
Cyberattacks	20
<b>Crime categories with elements of three types of crime infrastructure</b>	<b>20</b>
Crime directed at the welfare systems	20
<b>Criminal services and enablers</b>	<b>22</b>
<b>The most serious threats affect society's critical assets</b>	<b>24</b>
<b>Organised crime groups exploit society's vulnerabilities</b>	<b>26</b>
Trust and insufficient checks	26
Digitalisation enables anonymity and scalability	26
Insufficient information sharing between government agencies	27
The international dimension	27
Process-based societal systems slow down change	27
<b>Resilience and decisive action</b>	<b>28</b>
<b>Shifting effects</b>	<b>30</b>
Shift towards other forms of association	30
Crime shifting between countries	30
Shift towards increased use of bogus documents and identities	30

# Summary

The 2025 Cross-agency Situation Report presents the most serious threats and vulnerabilities related to organised crime. The 2025 report is based on documentation available within the framework of cross-agency work concerning criminal networks, areas of crime and factors in the world around us. One premise for this work is that the most serious threats are present in crime categories where there is considerable activity on the part of organised criminal networks – networks that have the capacity to threaten society's critical assets.

## Organised crime is a broad and complex problem

Organised crime in Sweden is flexible and diverse, and it involves both structured criminal schemes carried out over time and organised criminal networks with the capacity to threaten society. Crime occurs throughout the country, and the criminal actors in organised crime are active in most crime categories.

There is a great deal of variety in terms of how criminal actors are organised and how they conduct their criminal activity. Organised crime in Sweden is integrated into an international context. The criminal networks with the greatest capacity control the entire criminal chain of goods and services from country of production through smuggling to sales and use in Sweden.

Both criminal services and enablers are cogs in the machinery of organised crime, and almost all crime categories examined involve criminal services or enablers in some form or another. Criminal services are needed to carry out crime, and some criminal networks have specialised in selling one specific criminal service rather than carrying out the whole crime themselves. Money laundering and transport are the most obvious examples of criminal services, but there is a great deal of supply and a lot of variety. Put in simple terms, enablers are the people who make criminal services possible.

## The most serious threats affect society's critical assets

What distinguishes organised crime from other forms of crime is the criminal actors' ability to conduct criminal activity that threatens society's critical assets.

By using money laundering, criminal finances and legal business structures in their criminal activity, organised crime groups do not compete on a level playing field with serious actors and thus impact free competition in the economic sphere.

By using identity and document fraud, and exercising corruption or exerting unlawful influence, organised crime groups influence decision-making in our democratic society. The decisions of public authorities are then based on false premises, and this further distorts free competition and creates injustices in the welfare systems.

By using violence and intimidation, organised crime groups affect the physical safety of citizens.

Organised crime groups have the ability to circumvent the measures implemented by public authorities to detect and prosecute criminal activity.

The ability of criminal actors to threaten society's critical assets can be termed 'crime infrastructure'. The greatest threat from organised crime is in the crime categories in which the crime infrastructure features.

The following crime categories have elements of all types of crime infrastructure:

- Drug-related crime
- Environmental crime
- Fraud
- Money laundering
- Organised theft
- Sanctions evasion

## Organised crime networks exploit society's vulnerabilities

Organised crime networks are skilled at exploiting society's vulnerabilities to promote their criminal activity and maximise their criminal profits. For example, incorrect information in databases is used as a door opener for crime. When incorrect information is recorded at a government agency, it is then spread, as government agencies trust each other's databases and do not always share additional information that would contradict the information recorded. Digitalisation offers anonymity in that there are no physical meetings, and this reduces government agencies' possibilities to carry out checks. This opens up the door to crime. Digitalisation has also made it possible to scale up and increase volumes in crime. The international dimension of organised crime is a vulnerability due to the shortcomings in international information exchange. These shortcomings are exploited to cover up crime proceeds and for criminal schemes in the area of international trade.

The Government's strategy against organised crime,

Resistance and decisive action, aims to reduce the vulnerabilities exploited by organised crime and increase government agencies' room for manoeuvre.

## Organised crime networks are flexible and adaptable

Organised crime networks are flexible and quickly adapt to new or changing circumstances. The measures taken by government agencies affect organised crime groups and change their approach. The national strategy against organised crime and the measures taken by government agencies to combat organised crime are therefore expected to lead to a situation in which criminal networks are more likely to:

- exploit forms of association other than businesses in their criminal activities, such as foundations and non-profit organisations;
- exploit legal business structures and accounts in other countries;
- commit document and identity fraud; and
- reside in and commit offences from other countries.



# Introduction

## The cross-agency initiative

Following decisions by the Government<sup>1</sup>, there is now collaboration against organised crime between the Swedish Public Employment Service, the Swedish Economic Crime Authority, the Swedish Social Insurance Agency, the Swedish Prison and Probation Service, the Swedish Enforcement Authority, the Swedish Coast Guard, the Swedish Migration Agency, the Swedish Pensions Agency, the Swedish Police Authority, the Swedish Tax Agency, the Swedish Security Service, Swedish Customs, the Swedish Payments Agency and the Swedish Prosecution Authority. This work will henceforth be referred to as the cross-agency initiative against organised crime and the agencies involved will be referred to as the collaborating agencies.

With the exception of the Swedish Prosecution Authority, the collaborating agencies are represented in regional intelligence centres and in the National Intelligence Centre which is responsible for producing a Cross-agency Situation Report every other year. As in previous years, the 2025 Cross-agency Situation Report provides background material for the focus of the cross-agency initiative against organised crime.

## About the report

The purpose of the 2025 Cross-agency Situation Report is to present the most serious threats and vulnerabilities related to organised crime. The report is based on, among other things, intelligence that Sweden has contributed to Europol's threat assessment of organised crime in the EU, SOCTA<sup>2</sup> for 2025. The material includes documentation about criminal networks, areas of crime and factors in the world around us. Additional material, also in the form of situational reports and other reports from various government agencies and the regional intelligence centres, have also been used

as background material for the 2025 Cross-agency Situation Report.

The 2025 Cross-agency Situation Report is not an exhaustive situational report of all aspects of organised crime in Sweden. The report compares different crime categories based on a limited number of key perspectives in order to identify the most serious threats. One point of departure has been that the most serious threats are found where organised criminal networks are active, i.e. crime categories with strong elements of organised crime.

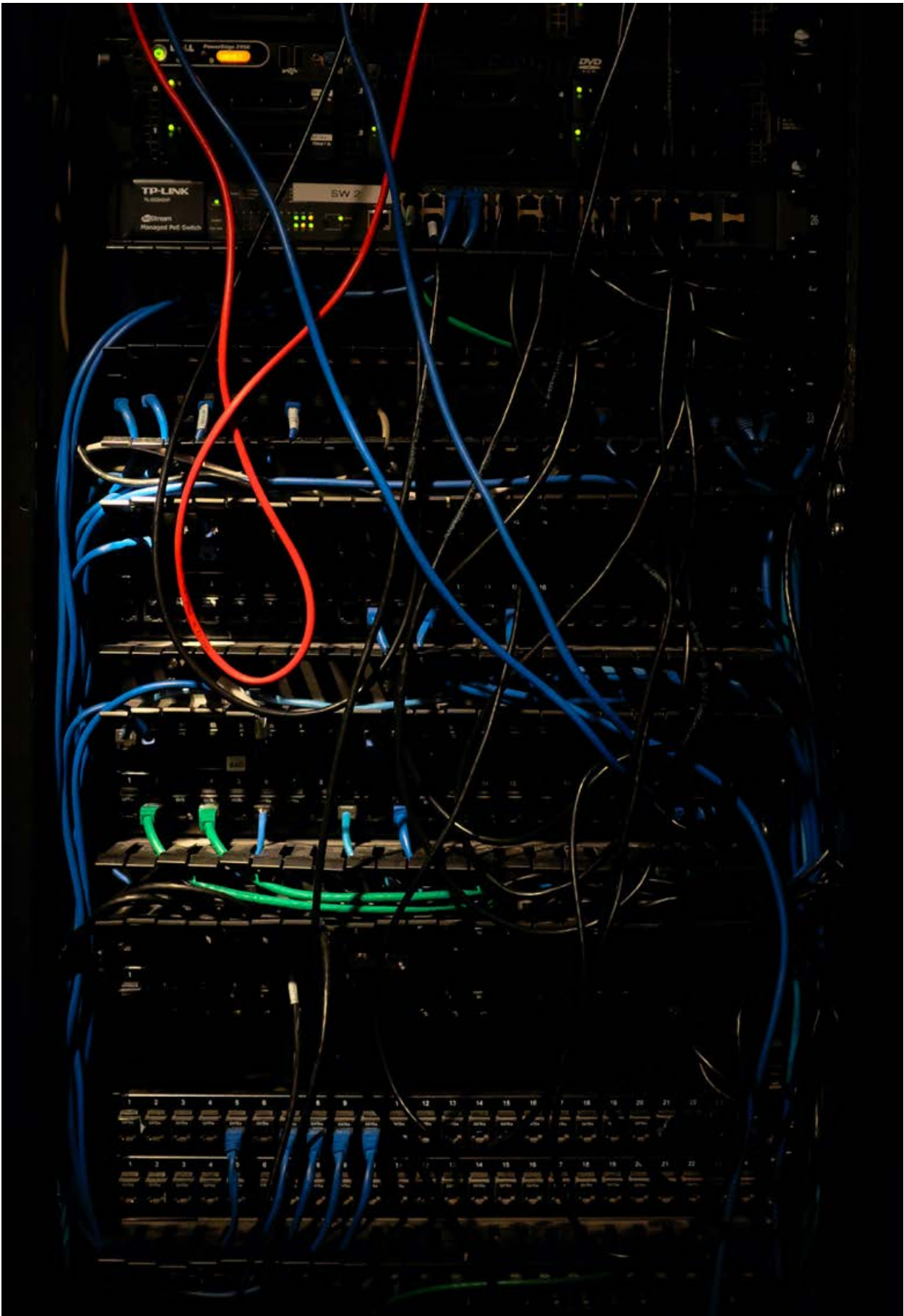
## The structure of the report

The report begins with a description of criminal networks in terms of number, the way they are organised and what kind of crime they are involved in. This is followed by a section describing the methods and strategies used by criminal actors and how these affect society's critical assets. Then there is a description of ten crime categories that are considered to affect several government agencies, cause major damage to society in Sweden and have documented elements of organised crime. After that there is a description of how organised crime groups use criminal services and enablers to carry out offences. The report concludes with a description of the most serious threats and vulnerabilities, how the national strategy against organised crime corresponds to the situation report, and how organised crime groups may adapt their approach in view of the national strategy.

---

<sup>1</sup> Ju2008/5776/PO and Ju2015/09350/PO

<sup>2</sup> Serious and Organised Crime Threat Assessment, SOCTA.





# Organised crime is a broad and complex problem

In summary, it can be said that organised crime is a broad and complex problem with a great deal of variation. It is present throughout Sweden, but with a certain level of concentration in the metropolitan areas. This report uses the EU's definition of organised crime. It is a broad definition that covers both structured criminal schemes and criminal networks with a great threat capacity. At the broader end of the spectrum, for example, we find environmental activists and supporter clubs, which are not traditionally seen as belonging to organised crime, yet they fall within the EU's broad definition. At the other end of the spectrum, we find criminal networks with a great threat capacity and international links. It is difficult to paint an exact picture of how extensive organised crime in Sweden is, but there are some indications that somewhat more than 62 000 people are involved, a figure stated by the Swedish Police Authority in early 2024<sup>3</sup>. The ways in which people are recruited to criminal networks vary, but one difference since the 2023 report is that there is a clearer trend towards the recruitment of young people. Some young people are recruited from residential care homes for children and young people, where the owners or staff have links to organised crime, and some young people are recruited via chat groups where murder commissions are accepted by young people who do not have any links themselves to organised crime.

When it comes to the networks with the greatest threat capacity<sup>4</sup>, there is a lot of variety in terms of number of members and type of network, but it is more common for them to be hierarchical than loosely composed. Unlike loosely composed networks, hierarchical networks have a clear leadership structure. One example of a hierarchical network is a family-based network. Common to many of the networks with the greatest threat capacity is also that they have been

## Fact

### Characteristics of organised crime

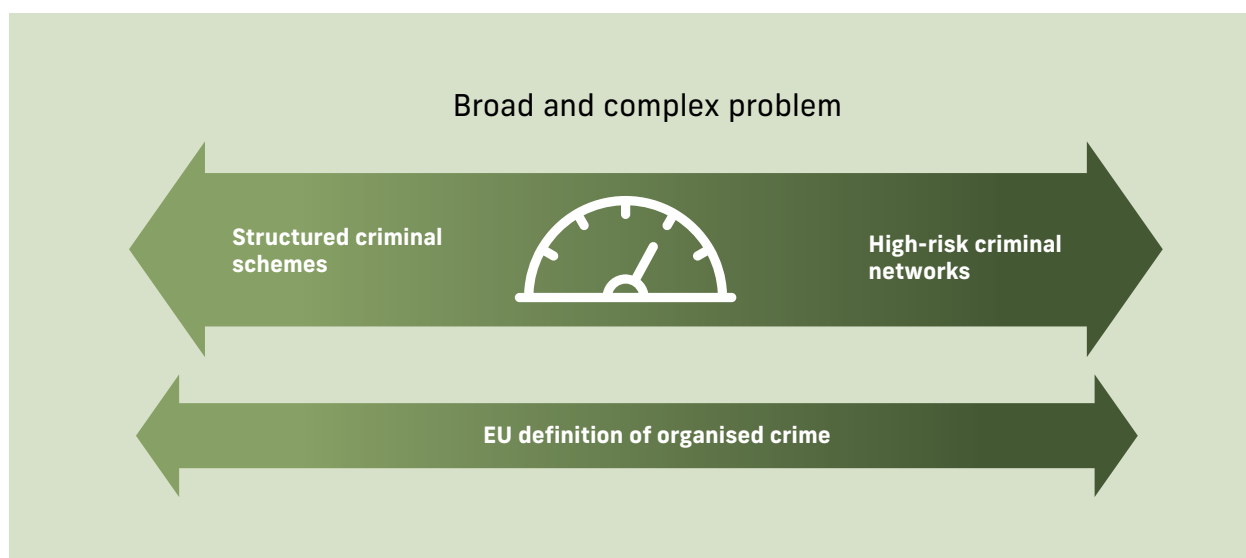
To classify organised crime, the 2025 Cross-agency Situation Report uses the EU definition of organised crime. At least six of the following characteristics have to apply, four of which must be those numbered 1, 3, 5 and 11, for any crime or criminal group to be classified as organised crime.

- 1. Collaboration of more than two people;**
- Each with own appointed tasks;
- 3. For a prolonged or indefinite period of time;**
- Using some form of discipline and control;
- 5. Suspected of the commission of serious criminal offences;**
- Operating on an international level;
- Using violence or other means suitable for intimidation;
- Using commercial or businesslike structures;
- Engaged in money laundering;
- Exerting influence on politics, the media, public administration, judicial authorities or the economy;
- 11. Determined by the pursuit of profit and/or power.**

<sup>3</sup> Swedish Police Authority. Situational picture of active gang criminals in Sweden (in Swedish). Government assignment. 2024.

<sup>4</sup> This report uses the method produced by Europol to assess the threat capacity of criminal networks. The method includes threat indicators in the form of the use of legal business structures, corruption and unlawful influence, violence and intimidation, money laundering and countermeasures, but also indicators concerning collaboration with other criminals, the financial resources of networks, geographical spread and mobility, and continuity and resilience in criminal activity.





active for more than ten years and that they control legal businesses that are used for crimes, such as money laundering.

The criminal networks with the greatest capacity devote themselves to various types of crime, even though the crimes are interlinked in one and the same criminal strategy. The networks' criminal strategies typically include narcotics offences, money laundering, weapons smuggling and violence, all for the purpose of financial gain. Some networks have the criminal expertise within their network, others outsource it, for example financial advice.

Although the purpose is financial gain for the networks, there are overlaps between criminal networks and violent extremist circles, mainly at individual level. In some cases, there are more systematic collaborations, with violent extremists using the expertise of organised crime actors to handle illegal goods. There are also examples of state actors using the expertise of organised crime groups to carry out attacks and at the same time deny their own involvement. The link to state actors is already known,<sup>5</sup> but it featured again in 2024 in connection with the violent incidents at the Israeli Embassy in Stockholm.

## Crime infrastructure

Crime infrastructure refers to the methods that organised crime actors need to carry out their profitable criminal activity. The term 'crime infrastructure' was taken from the SOCTA methodology<sup>6</sup>, and the criminal methods included are:

## Example

### Recruitment of young people

The recruitment of children and young people for crime has in many ways moved from physical locations, such as the local square and the school playground, to the digital world of social media and encrypted messaging services. This means that no place is safe and that the problem of young people being recruited to commit serious offences is spread throughout society.

Criminals currently use social media to post criminal tasks for children and young people to carry out. These tasks may involve transporting weapons, money or drugs, shooting someone or setting off an explosion in a doorway.

Once the criminals have identified children and young people who are willing to carry out violent crimes, these children are then often asked to download the app Signal, where the conversation continues. Other apps also feature, such as Telegram.

Young people also actively look for channels and chatrooms where they can see current violent tasks.

<sup>5</sup> Swedish Police Authority. Cross-agency Situation Report. Organised Crime 2023. 2023.

<sup>6</sup> SOCTA stands for Serious and Organised Crime Threat Assessment, which is Europol's assessment of the threat of organised crime in the EU.

- Use of legal business structures in the criminal sphere<sup>7</sup>
- Money laundering and criminal finances
- Identity and document fraud<sup>8</sup>
- Corruption and/or unlawful influence
- Violence and intimidation
- Countermeasures to avoid detection and prosecution

### Example

#### Sophisticated schemes for evading detection

A network originating in the Balkans starts transport businesses in EU countries such as Slovenia, Slovakia, Hungary and the Czech Republic as part of a deliberate strategy to evade suspicions of drug smuggling. The network is engaged in the large-scale smuggling of medical drugs classified as narcotics, including Ksalol (benzodiazepine), from Serbia to Sweden.

The overall purpose of organised crime is to make a financial gain. In its striving to make a financial gain, organised crime is a parasite on society, but it has no intention of making society collapse. But the striving to make a financial gain affects society's critical assets, as the crime infrastructure enabling organised crime has an impact on:

- free competition in the economic sphere;
- the fundamental processes of the democratic form of government; and
- the physical safety of citizens.

For example, the use of legal business structures, money laundering and criminal finances affects free competition in the economic sphere. The use of false identities and documents, corruption and unlawful influence affects the fundamental processes of the democratic form of government, and in some cases free competition. Threats and violence affect the physical safety of citizens. Put simply, crime infrastructure is what differentiates organised crime from other forms of crime. The majority of components in crime infrastructure are also criminal offences. The components in crime infrastructure and the areas of crime therefore overlap in many cases.

## Coherent crime strategy

A term that is closely related to crime infrastructure is 'components in criminal strategy'. It is clear in the material for the cross-agency report that criminal networks combine several different offences in one coherent criminal strategy. There is one main profitable crime in criminal networks' strategies, but the other offences are carried out so as to enable or launder the proceeds from the main crime. For example, several criminal networks combine corruption, weapons smuggling, extortion, violence/murder and money laundering in a strategy that supports their profitable drug trafficking. Some components in criminal strategy overlap with crime infrastructure.

The material showed that the following offences function as enabling components in criminal strategies:

- Corruption
- Extortion
- Kidnapping
- Identity and document fraud
- Illegal trade in weapons and explosive goods
- Staying in the country on false grounds
- Tax offences
- Accounting offences
- Criminal finances and money laundering

There are examples of criminal networks that sell these components as a service to other criminal networks. It is therefore also possible to make a financial gain from the enabling components. For example, in the crime area 'illegal trade in weapons and explosive goods', there are criminal actors who sell weapons and explosive goods as a criminal service<sup>9</sup>. Also, in the area of corruption and document fraud, there are criminal actors who have specialised in only providing part of the service, such as the material for false documents.

In several crime areas where legal business structures are used, tax offences and accounting offences are common occurrences as an integral part of criminal schemes. By creating accounts based on incorrect documentation and information, criminal actors can present a false picture of their business as legitimate and in some cases successful, thus making detection more difficult. Neglecting to report and pay taxes is one way of maximising criminal profits in these criminal schemes.

Just like crime infrastructure, the components in the criminal strategy affect society's critical assets.

<sup>7</sup> Here, the term 'legal business structures' includes various types of businesses, such as limited companies, sole trading companies, trading partnerships, limited partnerships, religious communities, foundations and associations.

<sup>8</sup> Identity fraud refers to both the use of false identities and to the exploitation of others' identities. Document fraud refers to the use of both false documents and incorrect documents, such as incorrect invoices.

<sup>9</sup> Internationally, and primarily within the context of Europol, this is known as Crime as a Service, or CaaS.



Violence and intimidation as a result of extortion and the illegal trade in weapons damage the possibility of the State to ensure that individuals are not subjected to physical attack. Corruption and identity fraud affect both free competition in the economic sphere and the fundamental processes of the democratic form of government, for example in terms of the exercise of public authority. Tax and accounting offences also affect free competition. The violence that is committed as part of crime also represents a cost to society in the form of healthcare and law enforcement resources from the Police, the courts and the Swedish Prison and Probation Service. Extortion, violence and corruption contribute to the establishment of parallel structures in society and affect confidence in the State.

Despite the fact that the components in organised crime groups' criminal strategies affect society's critical assets, the components do not generally require any great expertise, although there are examples of more sophisticated schemes. It is rather the criminal actors' ability to combine the different components in their criminal strategy to support their profit-driven

crime that is sophisticated.

The components in the criminal strategies are linked to the profitable crime areas they enable. Extortion, illegal trade in weapons and kidnapping have the clearest links to violence and drug trafficking. Corruption features mostly in connection with money laundering and criminal finances, but also when criminal actors promote their own profit-driven crime. Various forms of identity and document fraud are used in people smuggling, trafficking in human beings and exploitation of labour.

The components in the criminal strategies are used throughout the country. However, illegal trade in weapons and explosive goods is concentrated to the metropolitan areas and southern Sweden. Analyses carried out by the Swedish Police Authority show that vulnerable areas have a higher concentration of offences such as shootings, obstructing the course of justice and making unlawful threats than the rest of the country.

## Criminal finances and money laundering

Criminal finances and money laundering are the most common components in a criminal strategy and they are essentially needed in all criminal strategies. Criminal finances can be described as an ecosystem in which criminal profits are generated, handled and reinvested. Money laundering is therefore part of criminal finances. Criminal finances are thought to generate between SEK 100 billion and SEK 150 billion per year, and it is estimated that approximately SEK 130 billion is laundered each year in the Swedish financial system. A lot of the crime proceeds in criminal finances are achieved through tax offences, benefit fraud, fraud, waste crime and drug trafficking.

Criminal finances and money laundering function as a support for other crime and are a prerequisite for organised crime groups to be able to make use of crime proceeds. Criminal finances and money laundering have a negative impact mainly on the economic sphere, both in the private and public sector, partly in the form of a larger shadow economy, lost tax revenue, distorted competition and increased costs for the control activities of government agencies.

The majority of the criminal networks analysed are involved in criminal finances and money laundering. There is information to suggest that several criminal networks use professional money laundering actors and that the networks share logistics with each other, such as the transportation of cash. There is information about links between Russian-speaking organised crime groups in working life that need cash to pay for undeclared labour, and other criminal networks that need to get rid of cash.

### Example

#### Capital injections in companies to launder money

Investing capital in a company, for example in the form of additional investments from shareholders, new share issues and loans, is nothing unusual per se. Describing deposits of crime proceeds in company accounts as these kinds of capital injections makes the payments appear legitimate. The money can then be paid as salaries, dividends or false repayments of debts, and can therefore appear to have been obtained by legitimate means.

### Fact

#### TBML

Trade-based money laundering involves crime proceeds being concealed and moved through trade transactions so that the crime proceeds appear to have been obtained by legitimate means. This is done by giving false descriptions of the price, quantity or quality of goods. Trade-based money laundering is often referred to using the acronym TBML.

It is common for criminal networks active in the area of criminal finances and money laundering to have their own legal business structures or to infiltrate legal business structures. There are different ways to launder money using these business structures, for example triangle money laundering through factoring companies, consulting companies or invoice companies. Other ways to launder money through legal business structures include additional investments from shareholders that legitimise the extra capital in the company, fictional debts and incorrect personal details. Money laundering through cash-intensive businesses and trade-based money laundering (TBML) are other examples of how legal business structures are used.

Criminal actors can also exploit company bankruptcies as part of their criminal activity. Credit fraud and asset stripping detected through bankruptcies generate billions of kronor in crime proceeds every year. Bankruptcies can also be used to exploit the wage guarantee.

Sometimes criminal networks combine different money laundering schemes by alternating between using money couriers and carrying out company-related bank transactions, for example. Both demand for and supply of money laundering have increased in terms of cryptocurrency, partly because of the anonymity offered by crypto-assets. But despite the increased focus on crypto-assets, cash is still common in money laundering schemes, for example through the use of money couriers. Organised crime groups' money laundering is international in several regards. Hotspots<sup>10</sup> for money laundering include Tallinn, Dubai, London, Hong Kong, Istanbul and the Spanish Costa del Sol.

<sup>10</sup> Hotspots are a criminological term to describe an area specifically affected by crime.



# Crime areas

The analyses in this report are based on some 50 crime areas that form the basis of Sweden's reporting to Europol in connection with the Serious and Organised Crime Threat Assessment (SOCTA). The analyses were also supplemented with reports from the government agencies involved in the cross-agency initiative against organised crime, as well as open sources.

In the first stage of analysis, a number of crime areas were removed. The crime areas that were excluded from further analysis primarily concerned one single government agency, were not thought to cause any serious damage to Swedish society or there was no documented organised crime element involved. In the next stage of analysis, the remaining crime areas were divided into ten overarching crime categories. It is these overarching crime categories that are described in this report. Some of the crime areas were considered to be components in criminal strategies, and they are outlined in the section 'Coherent crime strategy'.

Each crime category has been analysed on the basis of:

- impact on society;
- estimated crime proceeds;
- presence of organised networks;
- crime infrastructure indicators;
- need for expertise;
- level of sophistication within the crime category; and
- possible regional and international dimension.

The crime category texts are therefore not exhaustive descriptions; instead, they are analyses from the perspectives listed above. In-depth information can be found in the government agencies' own reports on each crime category.

The crime categories are organised according to presence of crime infrastructure. Those crime categories with elements of all parts of crime infrastructure

are set out first. More overall information about crime infrastructure is contained in the section 'Crime infrastructure'.

## Crime categories with elements of all types of crime infrastructure

### Drug-related crime

Drug-related crime has a broad impact on society. For individual users, the damage to health is tangible and, in the worst case, deadly. For society, this means increased healthcare costs. Drug-related crime also brings with it criminal conflicts involving gun violence and explosives, which also risk affecting third parties. Moreover, drug-related crime leads to corruption of port staff and infiltration of law enforcement agencies. In Belgium and the Netherlands, for example, there is also an environmental impact, above all with regard to precursors<sup>11</sup> for synthetic drugs that are dumped in the natural environment post-production. Similar cases are yet to be detected in Sweden.

The drug market in both Europe and Sweden appears to be resilient in relation to the events that have happened around the world in recent years; in Sweden, the prices of several types of drug are at a historic low, and compared with 2019 drug prices are relatively unchanged, despite the fact that the period has been marked by high inflation, we have had a pandemic, and encrypted platforms have been cracked.<sup>12</sup> The Swedish Police Authority estimates that between 100 and 150 tonnes of drugs are smuggled into Sweden each year. It is difficult to calculate the turnover on the drug market in Sweden. Total turnover in Sweden in terms of hidden drug trafficking on the internet was estimated to be between SEK 700 million and SEK 1 billion in 2020. This figure is thought to account for 10 per cent of the total turnover of drug trafficking in Sweden.

<sup>11</sup> Substances that can be used in the illegal production of drugs.

<sup>12</sup> Developments in drug prices in Sweden 1988–2023 (in Swedish), Swedish Council for Information on Alcohol and Other Drugs, 2024.

Smuggling and sales of drugs are key to organised crime in Sweden, particularly among the established criminal networks with major threat capacity. In drug-related crime, project-based crime that is committed through temporary collaboration for a limited period is a common occurrence. In Sweden, there are criminal networks that control the entire crime chain, from production to sales, but there are also criminal networks that focus purely on one part of the crime chain, such as the sale of drugs.

The crime category ‘drug-related crime’ has elements of all types of crime infrastructure.

Crime infrastructure indicators – drug-related crime	
✓	Use of legal business structures
✓	Money laundering and criminal finances
✓	Identity and document fraud
✓	Corruption or unlawful influence
✓	Violence and intimidation
✓	Counter-measures

Organised crime groups use legal business structures as part of their drug-related crime; for example, transport companies are used for smuggling drugs. Legal business structures are also used to launder crime proceeds from drug-related crime. False identities and documents are used in such a way that criminals in this crime area have several identities, making it more difficult for law enforcement agencies to take action when international alerts are issued. The use of false identities can also be seen as a countermeasure by criminals to reduce the risk of detection. Unlawful influence is exerted through bribing port staff, for example. Violence is used against rival criminal actors.

Drug-related crime occurs throughout Sweden, but drug prices are generally lower in the metropolitan counties and in southern Sweden, even though the trend is towards lower price differences throughout the country. A more even price range indicates that this kind of crime has become established throughout the country and that the differences between the metropolitan areas and the rest of the country are disappearing.

The Swedish Police Authority and Swedish Customs consider that a large share of these drugs is smuggled into Sweden via the Öresund Bridge and Swedish ports. In Sweden, a number of towns and cities have

been identified as logistical centres for the storage, division and packaging of drugs. The major cities of Stockholm, Gothenburg and Malmö are thought to be the most important logistical centres from which drugs are distributed to several other regions, but there are logistical centres throughout the country.

Example

Ports as logistics hubs for drug smuggling

In April 2024, a record quantity of cocaine was seized at Norvik port in Nynäshamn. The Swedish Police and Swedish Customs found 1.3 tonnes of cocaine in a container with a street value of up to SEK 1.2 billion.

The majority of the drugs consumed in Sweden are imported to the country, but there is some domestic production on a small scale, primarily of cannabis and synthetic drugs. Sweden is also used as a transit country for drugs, en route to our neighbouring countries, for example. In recent years, Swedish criminal networks have become established in the drug markets in Norway and Finland. Swedish and Danish criminal networks cooperate on drug smuggling. So as to obtain control over a large part of the smuggling chain, Swedish criminals have long been established in regional smuggling hubs, such as Spain and Morocco.

Environmental crime

Environmental crime carries with it the risk of damage to air, land and water quality, as well as health risks, both now and in the future. In addition, this kind of crime creates unfair competition for serious actors. There are no reliable estimations of the total crime proceeds in the area of environmental and waste crime, but some believe them to be on a par with those of drug trafficking.

Offences include the illegal handling, storage and export of hazardous waste, plastics and electronics, and scrap vehicles. It is not known how many criminal networks commit environmental crime, but it is clear that there are networks with a major threat capacity that are active in this crime category. This kind of crime is committed as part of business activities, and the actors committing environmental crime can be linked to economic crime, work environment crime and trafficking in human beings.

All types of crime infrastructure feature in the crime category ‘environmental crime’.

### Crime infrastructure indicators – environmental crime

- ✓ Use of legal business structures
- ✓ Money laundering and criminal finances
- ✓ Identity and document fraud
- ✓ Corruption or unlawful influence
- ✓ Violence and intimidation
- ✓ Counter-measures

Legal business structures often feature in waste crime, for example export and import companies, waste management companies and consulting companies. Legal business structures are also used for trade-based money laundering of crime proceeds. False documentation and identities are used to avoid detection in customs checks. Corruption and infiltration are used to promote criminal activities and evade checks, and violence and intimidation are sometimes also used as part of corruption and infiltration.

Environmental crime occurs throughout Sweden, but most cases are detected close to large towns and

### Example

#### Think Pink

NMT Think Pink AB and its subsidiary Resurs-Recycling i Stockholm AB were exploited in the highly publicised case known as the ‘Think Pink affair’. Of the eleven people charged in total, two former managing directors, one waste broker, one location manager and one environmental consultant were found guilty by the District Court in June 2025 of gross environmental offences and sentenced to imprisonment, suspended sentences and fines. Five persons were found guilty of environmental offences and sentenced to imprisonment, suspended sentences and fines. Four of the eleven people were also charged with gross accounting offences, gross dishonesty to creditors and gross breach of trust. The charges concerning the economic crime have not yet been examined by a court.

cities. Waste is exported illegally from Sweden to various parts of Africa and the Middle East. Sweden is sometimes also a transit country for waste coming from Norway that is then transported to the Baltics. In addition, waste is sometimes imported from Norway, Finland, Denmark, the United Kingdom and Italy, and these imports have links to criminal networks.

### Fraud

Fraud causes increased costs for insurance and security, and personal trauma for those affected, and it contributes to the shadow economy. The Swedish Police Authority estimates that fraud generated approximately SEK 7.5 billion in crime proceeds in 2023<sup>13</sup>.

Many of the individuals who are active in various forms of fraud are also involved in other crime, and the crime proceeds from fraud are reinvested in drugs and weapons. Statistics on fraud and serious violent crime have correlated in recent years. However, it is not clear why the trend for fraud and serious violent crime is so similar.<sup>14</sup>

All types of crime infrastructure feature in the crime category ‘fraud’.

### Crime infrastructure indicators – fraud

- ✓ Use of legal business structures
- ✓ Money laundering and criminal finances
- ✓ Identity and document fraud
- ✓ Corruption or unlawful influence
- ✓ Violence and intimidation
- ✓ Counter-measures

Legal business structures can be used to commit fraud. For example, marketing companies with online activities can be used to send out a large number of text messages to deceive the recipients. Legal business structures are also used to launder crime proceeds from fraud in various trade-based money laundering schemes. Violence is rarely an integral part of these criminal schemes, but violence and intimidation are sometimes used against strawmen in the money laundering part of the scheme.

Sometimes crime victims’ electronic ID is manip-

<sup>13</sup> Crime proceeds from fraud in 2023 (in Swedish), Swedish Police Authority 2023.

<sup>14</sup> Organised fraud. A report on fraud linked to organised criminal circles (in Swedish), Swedish Police Authority 2021.

ulated so that criminal actors can buy goods using the victim’s identity or take out a loan in their name. There are also examples of bank staff having been corrupted so that they will assist in criminal schemes.

To avoid detection and prosecution, criminal actors submit freedom of information requests for investigations so that they can learn how crimes are investigated by the authorities.

Fraud is prevalent throughout the country. Various types of fraud<sup>15</sup> require different levels of organisation and complexity, but on the whole, they require expertise for fraudulent offences to be carried out successfully.

The clearest international element of fraud is the laundering of crime proceeds, which often takes place using international payment services. A money laundering cluster has been identified in Spain, in the region around Marbella and Malaga. From both phishing fraud (BEC)<sup>16</sup> and romance fraud, there is a flow of crime proceeds to Nigeria and West Africa.

**Organised theft**

Organised theft in the form of the theft of vehicles and spare parts, technical equipment from construction and agricultural machinery, and boat engines, is a profitable crime category for organised crime groups. Aside from the financial value of stolen products, organised theft leads to reduced confidence in government agencies, a sense of reduced safety and higher insurance premiums. Thefts of diesel and machines from building sites or forestry sites also affect individual businesses. There is no coherent assessment of the value of the goods stolen by international crime networks, but Larmtjänst<sup>17</sup> estimates that insured goods are stolen in Sweden each year to the tune of several billion kronor.

Several hundred international crime networks have been active in Sweden since the early 2020s, and several networks with major threat capacity engage in organised theft. These networks are from countries in South America, Romania, Lithuania and Poland, and Russian-speaking countries, among others. A lot of the money generated in Sweden probably flows back to the networks’ countries of origin.

All types of crime infrastructure feature in the crime category of ‘organised theft’.

Crime infrastructure indicators – organised theft	
✓	Use of legal business structures
✓	Money laundering and criminal finances
✓	Identity and document fraud
✓	Corruption or unlawful influence
✓	Violence and intimidation
✓	Counter-measures

To commit organised theft, criminal actors use legal business structures that are registered to anchors or strawmen. They launder money using false invoices and use different identities and false ID documents. To gather information about law enforcement methods, they use enablers, and to avoid detection and prosecution they use jammers, hidden accommodation and name changes. Unlawful influence takes place in the form of insiders sharing information with the criminal actors, and this features in transport and logistics businesses, as well as in some cases at law enforcement agencies. Criminal actors will sometimes threaten and use violence against people in the margins of the criminal network, such as drivers and enablers.

International crime networks are active all over the country, but there are clear clusters in the metropolitan regions and along the natural transport routes, above all the E6 motorway between Malmö and Gothenburg and on towards the Norwegian border, the E18 motorway between Karlstad, Stockholm and Norrtälje, and the E4 motorway from Stockholm to Gävle, Sundsvall and further north to Umeå and Haparanda. Polish criminal networks are most strongly established in Police Regions South and West, the Romanian networks in Police Regions West and Stockholm, the South American networks in Police Region Stockholm, and the Lithuanian networks are relatively evenly established throughout the country.

15 The Swedish Police Authority uses the following categories in its analyses of fraud: advertisement fraud, identity fraud, card fraud, social manipulation, invoice fraud, cheating, gross claims fraud and insurance fraud, benefit fraud and other forms of fraud.  
16 Business Email Compromise (BEC) is a type of phishing fraud aimed at bringing about direct transfers of money or accessing sensitive information.  
17 Larmtjänst is an industry organisation that combats insurance-related crime and supports insurance companies’ investigations concerning uncertain insurance cases. Larmtjänst compiles information about what goods have been reported lost, when and how.



**Sanctions evasion**

Sanctions are foreign and security policy tools imposed by either an individual state or an intergovernmental organisation. Sweden has committed to following the sanctions regimes adopted by the UN and the EU. In total, Sweden is bound by some forty sanctions regimes. These can mainly be found in EU regulations, which are directly applicable as Swedish law. Sanctions involve restrictions in the freedom of action of a State, region or group, or of an individual. Russia’s war of aggression against Ukraine has led several countries in the Western world, including the EU, to considerably increase the number and scope of sanctions against Russia and actors helping Russia.<sup>18</sup>

State actors, such as Russia and Iran, use complex, cross-border business schemes to avoid detection or in some other way evade sanctions and thus strengthen their ability to carry out security-threatening activities against Sweden and other Western countries. The intelligence and security services of foreign powers can play a decisive role in the design of such business schemes, above all when it comes to products with military areas of use. It is not known how large the sums involved in illegal, indirect trade and the evasion of sanctions are. There are a number of criminal actors in Sweden who breach the sanctions regimes Sweden is bound by, including actors with links to the intelligence and security services of foreign powers.

All types of crime infrastructure feature in the crime category ‘Sanctions evasion’.

Crime infrastructure indicators – sanctions evasion

✓ Use of legal business structures

✓ Money laundering and criminal finances

✓ Identity and document fraud

✓ Corruption or unlawful influence

✓ Violence and intimidation

✓ Counter-measures

The ability of foreign state actors to avoid detection and evade sanctions is dependent on a number of methods that are common in crime infrastructure. These actors use trade-based money laundering,

letterbox companies, cryptocurrencies and enablers in criminal finances to conceal their often complex criminal schemes. Money couriers, hawala businesses and the use of neobanks make it even more difficult to detect and prevent the circumvention of sanctions provisions. Unlawful influence, such as making unlawful threats, influence campaigns and to some extent violence are also used to enable breaches of sanctions provisions. One particular challenge in terms of trade sanctions is that goods tend to be transported between several different jurisdictions inside and outside the EU. This makes traceability and control more difficult for both operators and law enforcement agencies. The use of false or manipulated documents linked to import and export makes follow-up even more difficult.

**Crime categories with elements of five types of crime infrastructure**

**Excise fraud**

Just like with VAT fraud, excise fraud tends to involve independent, profitable criminal schemes. Excise duty is consumption tax levied to influence the consumption of products that are environmentally hazardous or harmful to people’s health. Excise fraud involving alcohol, oil and tobacco can be linked to organised crime.

Excise fraud leads to tax shortfalls, unfair competition and an increase in criminal finances. Excise fraud involving tobacco can also result in a negative impact on health as the tobacco products are not quality assured. It is difficult to gauge how large the crime proceeds from excise fraud are, but the Swedish Tax Agency estimates that the tax shortfall due to excise fraud involving alcohol in 2021 was SEK 1.2 billion, and SEK 200 million for tobacco. It is not known what proportion of the tax shortfall is caused by organised crime groups.

Several criminal networks are active in the area of excise fraud. Criminal networks active in the area of excise fraud involving tobacco are sometimes also active in cannabis crime, alcohol-related excise fraud and identity-related crime. Carousel trade also occurs with goods subject to excise duty. Networks sometimes work with each other and adapt quickly to changes. The level of expertise is high, although this expertise differs depending on whether the fraud involves alcohol, tobacco or oil.

There are five types of crime infrastructure that feature in the crime category ‘excise fraud’.

<sup>18</sup> <https://www.government.se/government-policy/foreign-and-security-policy/international-sanctions/>, Swedish Government Offices, 03.10.2024

CROSS-AGENCY SITUATION REPORT, 2025 | 17

### Crime infrastructure indicators – excise fraud

- ✓ Use of legal business structures
- ✓ Money laundering and criminal finances
- ✓ Identity and document fraud
- Corruption or unlawful influence
- ✓ Violence and intimidation
- ✓ Counter-measures

Criminal actors use legal business structures to launder money and to issue invoices and sell goods to serious actors.

Money laundering is largely cash-based when it comes to tobacco. Money from alcohol- and oil-related excise fraud is laundered using sophisticated methods, such as trade-based money laundering.

Criminal actors control other people's identities and place them as representatives of the legal business structures.

Some networks that engage in excise fraud use violence and threats of violence when conflicts occur within the network.

It is primarily the metropolitan regions of Malmö and Stockholm that are the hubs for this kind of crime. The ports at Nynäshamn, Karlshamn, Trelleborg, Kapellskär and Umeå are also hotspots, particularly ports with traffic coming from the Baltics. The border between Haparanda and Finland, and border crossing points to Norway are also key to this area of crime. The manufacture of illegal products usually takes place in less densely populated places, such as areas close to the Norwegian border. There has been an increase in demand for goods due to industry initiatives in Skellefteå, Luleå and Boden. Several countries both within and outside the EU are involved in the criminal process for excise fraud, with a certain concentration in the Baltic countries.

### Organised crime in working life

Within organised crime, there are networks that operate in the area of working life. Criminal actors distort free competition in working life and at the same time fuel the criminal economy. The purpose of this type of crime is to generate and maximise profit by evading

taxes and exploiting labour, for example. The delegation to combat crime in working life estimates that undeclared income linked to crime in working life amounts to SEK 81–94 billion per year. It is not known what proportion of this figure can be put down to organised crime.

### Example

#### Thai berry pickers exploited

Seasonal berry pickers from Thailand were promised a salary in accordance with the Swedish collective agreement, meaning an 8-hour working day, but they were paid per kilo of berries they picked and worked for up to 17 hours a day. The perpetrators also withheld the berry pickers' passports so that they would not be able to work or sleep anywhere else. The perpetrators were convicted of gross human exploitation and sentenced to imprisonment and a seven-year trading prohibition.

Russian-speaking organised crime groups and family-based criminal networks are prominent in this area, and several criminal networks with major threat capacity engage in trafficking in human beings for labour exploitation.

There are five types of crime infrastructure that feature in the crime category 'organised crime in working life'.

Exploitation of legal business structures is a key part of crime in working life. For example, legal business structures are used to issue incorrect invoices and forge A1 certificates<sup>19</sup> that falsely state that employees are to pay social security contributions in their home countries and not in Sweden. To avoid detection, strawmen are registered on the company boards so that the criminal actors remain at a distance from the crime. There is an element of threats of violence against the exploited workers.<sup>20</sup> Laundering of cash occurs in this crime area.

There are regional differences depending on how well established the organised crime group is in the local business sector and individual industries. Larger projects, such as infrastructure initiatives and industrial projects, open up for legal business structures with links to organised crime, regardless of which region the infrastructure project is taking place in. The exploited workers come from countries such as Ukraine, Thailand, Uzbekistan and India. The businesses controlled by criminal actors are in countries such as Sweden, Thailand and Poland.

<sup>19</sup> An A1 certificate shows which EU/EEA country's social insurance system a person belongs to and governs where the employer is to pay social insurance contributions.

<sup>20</sup> See, for example, Crime in Working Life – a threat to positive productivity growth, Fi 2023:03 2024 (in Swedish).

#### Crime infrastructure indicators – organised crime in working life

- ✓ Use of legal business structures
- ✓ Money laundering and criminal finances
- ✓ Identity and document fraud
- Corruption or unlawful influence
- ✓ Violence and intimidation
- ✓ Counter-measures

#### VAT fraud

In the area of economic crime, VAT fraud is usually committed through independent, profitable criminal schemes. VAT fraud results in distorted competition, making it more difficult for serious actors to engage in the business sector, and loss of tax revenue, which ultimately affects the financing of the public sector. According to the most recent estimates in SOU 2024:32, this kind of fraud was thought to amount to SEK 5–6 billion per year in 2019 and 2020.

Several criminal networks with major threat capacity commit VAT fraud, and this kind of crime varies in its complexity. This kind of crime involves both acquisition fraud and carousel fraud. The actors trade in various kinds of goods, such as foodstuffs and electronic goods.

There are five types of crime infrastructure that feature in the crime category ‘VAT fraud’.

#### Crime infrastructure indicators – VAT fraud

- ✓ Use of legal business structures
- ✓ Money laundering and criminal finances
- ✓ Identity and document fraud
- ✓ Corruption or unlawful influence
- Violence and intimidation
- ✓ Counter-measures

Given that a VAT registration number is a prerequisite for committing VAT fraud, access to a legal business structure is necessary. It is primarily limited companies that are used in various ways and in countries such as Sweden, Germany, the Netherlands, Italy,

Poland and Hungary.

Criminal actors use alternative bank platforms in and outside the EU to launder money. They also launder crime proceeds through legal business structures and false invoices, and by investing in property. The money is mainly laundered in the United Arab Emirates, Sweden, Cyprus, Malta and Hong Kong.

Criminal actors use false documents such as incorrect invoices, fake transport documents and fake bank statements in their criminal activity.

There is information to indicate that unlawful influence is exerted as criminal actors have links to people who work at government agencies, banks and logistics companies.

Criminal actors adapt their schemes to avoid detection and prosecution, partly by changing the types of goods they trade in, switching countries for their trade and changing companies.

VAT fraud has a clear international dimension. Some countries feature more prominently than others, in terms of both where the legal business structures are located and where actors operate. The more prominent EU countries include Denmark, Germany, the Netherlands, Cyprus, Malta and Poland. Countries outside the EU that feature more frequently include Turkey, Lebanon, the United Kingdom and Pakistan. In terms of acquisition fraud and convenience goods and food, actors mainly operate in Denmark, Sweden, Lebanon and Turkey.

Logistics means that the prevalence of VAT fraud varies across Sweden. VAT fraud is more frequent in southern and central Sweden, in places such as Gothenburg, Helsingborg, Malmö and Stockholm. Logistics centres for electronics are located in Stockholm and southern Sweden.

#### Fact

##### Acquisition and carousel fraud

VAT fraud can be divided into acquisition fraud and carousel fraud. Acquisition fraud is a simpler variety of VAT fraud. Acquisition fraud is when a fictitious company buys goods from another EU country and then sells these goods on at a low price to another company in its own country, deducting VAT.

Carousel fraud is a more sophisticated version of VAT fraud whereby the same goods are delivered numerous times to the same company in a transaction chain, without any VAT being paid to the State. This variety requires at least three actors in two EU countries to collaborate, with one of the companies being a fictitious company.

Crime categories with elements of four types of criminal infrastructure

Cyberattacks

Cyberattacks essentially impact all sectors of society, resulting in several different effects for both public sector actors and private individuals. For example, various kinds of payment systems may temporarily cease to function and critical infrastructure such as electricity and water supplies can be affected. It is difficult to estimate how large the crime proceeds are that are generated by cyberattacks in Sweden, but an estimate from the Confederation of Swedish Enterprise suggests that IT-related crime, which includes cyberattacks, generated SEK 2 billion in 2022.

The largest threat in the crime category ‘cyberattacks’ is what are known as ransomware attacks. Ransomware is a kind of malicious software that is used for extortion purposes. This is often done by files being taken ‘hostage’ through encryption. The actors behind cyberattacks are often outside of Sweden, and leading and enabling groups come from the former Soviet Union. The criminal networks that engage in cyberattacks are also involved in money laundering and online fraud.

There are four types of crime infrastructure that feature in the crime category ‘cyberattacks’.

Crime infrastructure indicators – cyberattacks

✓ Use of legal business structures

✓ Money laundering and criminal finances

✓ Identity and document fraud

○ Corruption or unlawful influence

○ Violence and intimidation

✓ Counter-measures

Criminal actors use legal business structures to gain access to IT infrastructure such as VPS and VPN<sup>21</sup>. False documents and identities are used to gain access to IT infrastructure. The money is laundered using crypto-assets, for example. Countermeasures to avoid detection and prosecution include advanced security

and measures to conceal infrastructure and money laundering flows.  
Cyberattacks occur throughout the country.

Example

Consequences of major cyberattack

In early 2024, the company Tietoevry was the victim of a ransomware attack, meaning that municipalities, private companies and government agencies experienced problems with their IT systems. One effect was that Västerbotten Region had difficulties discharging patients from hospitals and into municipal care as the region's patient discharge system stopped working during the cyberattack. The wage systems of approximately 120 government agencies were also temporarily out of action.

Crime categories with elements of three types of crime infrastructure

Crime directed at the welfare systems

Crime directed at the welfare systems affects confidence in the welfare systems as criminal actors abuse the system to the detriment of people who are entitled to welfare. When criminal actors who run legal business structures in the welfare sector do not pay taxes, fees or salaries, or fail to abide by other labour law rules and work environment law, they are able to keep their tenders low in public procurement processes and thus create unfair competition.<sup>22</sup> This crime generates large crime proceeds every year. In 2021, between SEK 13 billion and SEK 16.3 billion was paid incorrectly from the state welfare systems according to the latest figures from the Swedish National Financial Management Authority. Around 90 per cent is estimated to have been paid incorrectly due to people applying for financial support, and an average of 56 per cent of this is believed to be due to deliberate errors. It is not known what proportion of these errors is caused by organised crime groups.<sup>23</sup>

Welfare crime affects several government agencies that pay benefits, including the Swedish Public Employment Service, the Swedish Social Insurance Agency, the Swedish Migration Agency, the Swedish Pensions Agency and the Swedish Tax Agency, as well as municipalities and regions. Some welfare systems are particularly vulnerable, such as dental care sub-

21 Virtual private server, VPS, is a method for dividing up a physical server computer into several virtual servers. Virtual private network, VPN, is a technology used to create a secure connection or ‘tunnel’ between two points in a non-secure computer network.  
22 Resistance and decisive action – a national strategy against organised crime, Swedish Government Offices 2024.  
23 The scale of incorrect payments from the welfare systems (in Swedish), Swedish National Financial Management Authority 2023.





sides, the wage guarantee system, various forms of employer support and assistance allowance.<sup>24</sup>

Several criminal networks have individuals who are active in welfare crime, but it is difficult to assess whether the whole of a network is engaged in welfare crime or just individuals in the network. These networks are also active in labour exploitation and document and identity fraud. One example of the type of network where some individuals commit welfare crime is the family-based network.

Three types of crime infrastructure feature in the crime category 'crime directed at the welfare systems'.

As mentioned previously, criminal actors use legal business structures to commit welfare crime, including in the assistance sector. In addition to the participation in public procurement processes on unfair terms, legal business structures and non-profit organisations are also used to offer bogus employment and false certificates.<sup>25</sup> The false certificates function as a door opener to the welfare systems. Criminal actors also use unlawful influence to commit welfare crime.

Welfare crime is committed throughout the country, but there are clusters of criminal expert knowledge that spread and sell know-how about how benefits and support can be exploited, for example in the areas of assistance and dental care subsidies. However, there is information to suggest that most cases of assistance fraud occur in Region Stockholm and Region South.

#### Crime infrastructure indicators – crime directed at the welfare systems

- ☒ Use of legal business structures
- ☐ Money laundering and criminal finances
- ☒ Identity and document fraud
- ☒ Corruption or unlawful influence
- ☐ Violence and intimidation
- ☐ Counter-measures

<sup>24</sup> Resistance and decisive action – a national strategy against organised crime, Swedish Government Offices 2024.

<sup>25</sup> Organised crime – a situational picture (in Swedish), Swedish Public Employment Service 2024 and Situational picture of organised crime (in Swedish), Swedish Social Insurance Agency 2023.

# Criminal services and enablers

Both criminal services and enablers are cogs in the machinery of organised crime. Criminal services are needed to carry out offences and are included as part of the crime strategies. Criminal actors can sell or exchange criminal services with each other. Put in simple terms, enablers are the people who make criminal services possible.

Almost all crime categories investigated have some element of criminal services or enablers, which points to the key importance of criminal services for crime infrastructure. Measures against these services therefore have an effect in several different crime categories and represent a vulnerability to some extent for criminal groups.

In some crime categories, such as cyberattacks and fraud, it is possible to buy an entire criminal scheme, or parts of a criminal scheme, online. On the whole, parts of criminal schemes that are needed in several different types of crime category are developed into criminal services that are then provided to several different criminal networks.

Money laundering and transport are the most obvious examples of criminal services, but there is a great

## Criminal services and enablers



### Example

#### 'Invoice-writing factories' as a criminal service

One example of a criminal service is what are known as 'invoice-writing factories' in Russian-language organised crime. The scheme involves a criminal network invoicing a customer, which is often a construction company in need of cash to pay for undeclared labour, via a company for a fictitious job carried out. Once the money has been transferred in several stages via hundreds of companies using strawmen, the money finally ends up as cash with the company needing cash to pay salaries outside the transactions recorded in the accounts.

deal of supply and a lot of variety. Another example is the provision of legal business structures, and/or false identities and documents. This may also involve providing false certificates or failing to report an offence. Auditors, bank employees, accountants, bankruptcy trustees, lawyers, estate agents, trustees and interpreters are some examples of professional categories that act as enablers for criminal services.

Legal business structures and government agencies can be exploited in the framework of criminal services. There are examples of courts that are exploited for money laundering purposes through settlement cases concerning real and fictitious debts. Estate agents, preschools and health clinics have also been used to enable organised crime in Sweden.

Organised crime groups have various strategies when it comes to using criminal services. Some networks buy criminal services to be able to carry out their criminal schemes, whereas others choose to

develop know-how within the network and control all parts of the criminal scheme. There are also examples of criminal networks that both carry out criminal components for their own primary criminal activity and sell them as a service to other criminals. One example is the organising of sham marriages to create a legal façade for third-country nationals to stay in Sweden.

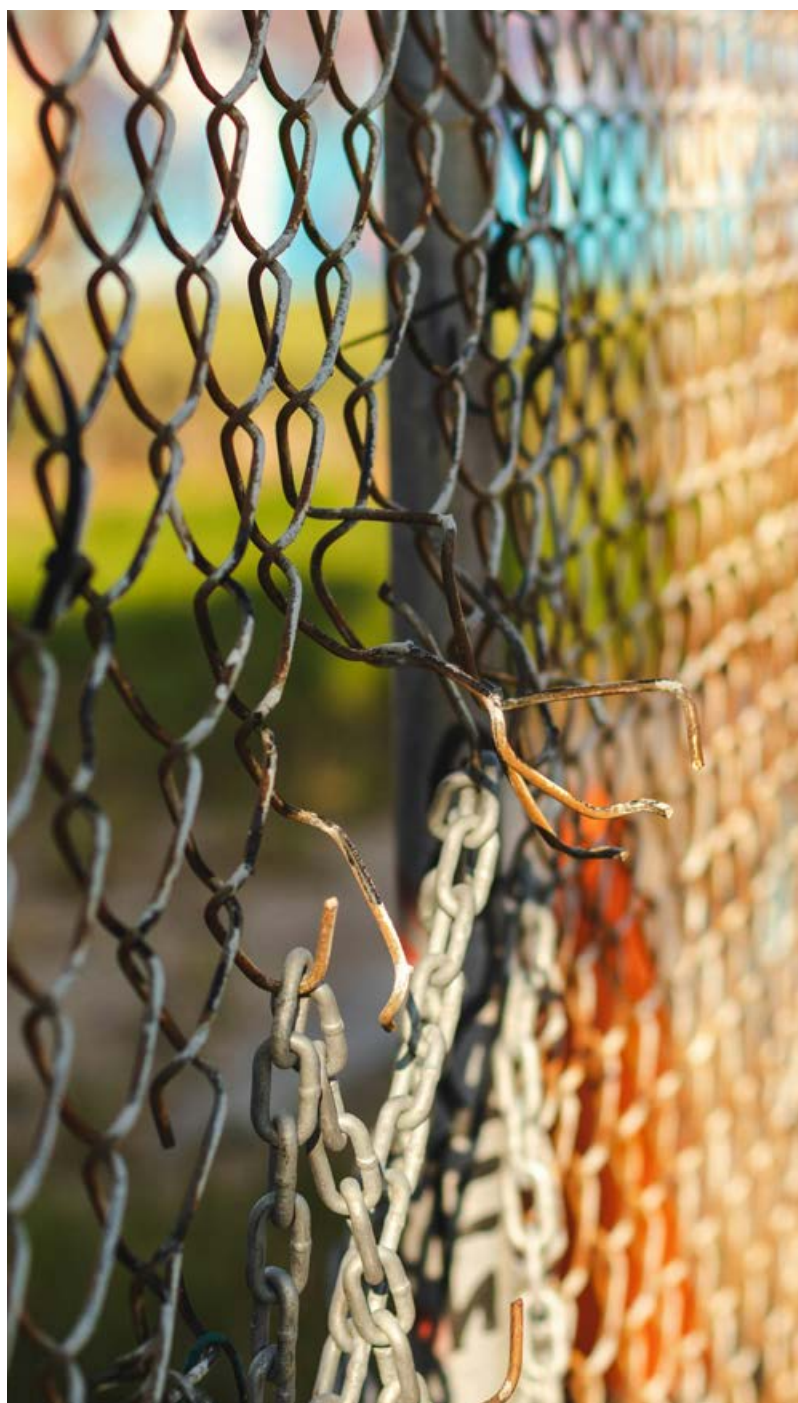
Criminal networks can also assist each other in exchange for payment when the need arises. In drug trafficking there have been examples of when the collection of drugs from a port, for example, has failed. The criminal network that has organised the drug smuggling will then advertise a general offer for someone to collect the drugs in exchange for payment.

### Example

#### Sham marriages

There are networks that both use and sell schemes giving third-country nationals without a Swedish residence permit the possibility to live and work here by creating false certificates of employment and offering sham marriages with other EU nationals who actually live in a different EU country.

Networks persuade EU nationals to travel to Sweden, become officially resident here, obtain a Swedish personal identity number or coordination number and a bank account, and enter into sham marriages with these third-country nationals in exchange for payment. All of this can be done in the course of one single day, after which the EU national travels back home. The sham marriage then gives the third-country national the possibility of obtaining a residence permit which provides better opportunities to reside and work in Sweden. The travel of EU nationals also gives networks access to their identities, which can then be exploited in future crime.



# The most serious threats affect society's critical assets

The most serious threat from organised crime groups is their ability to implement strategies that threaten society and target

- free competition in the economic sphere;
- the fundamental processes of the democratic form of government; and
- the physical safety of citizens.

As previously described, crime infrastructure enables organised crime. The crime infrastructure assessed within the framework of the Cross-agency Situation Report includes money laundering and criminal finances, legal business structures as part of organised crime, document and identity fraud, violence and intimidation, corruption or unlawful influence, and countermeasures. The following crime categories have elements of all types of crime infrastructure:

- Drug-related crime
- Environmental crime
- Fraud
- Money laundering
- Organised theft
- Sanctions evasion

This means that organised crime groups use all types of crime infrastructure that affect society's critical assets in these crime categories. The common occurrence of crime infrastructure in these crime categories makes them especially complex.

The criminal networks with the greatest threat capacity are active in all of the above crime categories, apart from sanctions evasion. However, none of the criminal networks with the greatest threat capacity that are active in organised theft have this as their main criminal activity.

The criminal networks with the greatest threat capacity are also active in crimes such as labour exploitation, benefit fraud, fraud linked to food and drink, document and identity fraud, illegal trade in weapons and explosive goods, kidnapping, corruption, betting-related crime, murder and gross assault, VAT fraud, human trafficking for sexual purposes and extortion.





# Organised crime groups exploit society's vulnerabilities

## Trust and insufficient checks

All of the vulnerabilities identified in the Cross-agency Situation Reports of 2019, 2021 and 2023 remain, although they have been reworded slightly in each report. Organised crime groups continue to exploit society's trust-based system, and this is combined with the fact that control systems have shortcomings. Vulnerability in terms of crimes against the welfare systems is clear, but vulnerabilities are also exploited in crime categories such as fraud, organised crime in working life, economic crime and environmental crime.

## Digitalisation enables anonymity and scalability

Digitalisation has resulted in greater anonymity, with the lack of physical meetings making it harder for government agencies to check people's identities and for victims to check who a message is actually from. Anonymity also helps make it easier for criminals to conceal their ownership or control of businesses and bogus identities used as crime instruments.

In the same way as Swedish government agencies, businesses and financial institutions have worked on service and digitalisation, so have other countries and their equivalent agencies worked on these issues. This means that the threshold for setting up a foreign company structure or foreign bank accounts, or obtaining help from foreign enablers, has become lower. Solutions that in the past would have cost a lot of money, been difficult to access and involved a heavy administrative burden have become cheaper and easier than before thanks to technological developments. Enablers contribute know-how for the administration of company structures, and provide formal representatives and addresses, and other services in several stages across national borders. The schemes,

### Example

#### Vulnerabilities linked to assistance allowance

The Swedish Health and Social Care Inspectorate and the Swedish Social Insurance Agency have noted that there are companies that function as administrators of personal assistance. Consultancy activities do not require a permit and companies can thus circumvent the supervision of the Inspectorate. This scheme also means that the company cannot be made to pay anything back to the Swedish Social Insurance Agency because repayment demands can only be made to the person who received the payment, i.e. the client. This is despite the fact that the company invoices the client for the full assistance allowance sum and administers the personal assistance.

which involve tailored financial instruments, special company structures and other solutions, are provided so as to circumvent international reporting<sup>26</sup> and limit transparency concerning ownership structures and insight for outsiders. This makes it more difficult for the authorities to carry out checks and it facilitates or enables tax offences and money laundering.

Digitalisation means that organised crime groups can scale up their criminal activity. Examples of this include when single invoicing entities have used hundreds of companies in a short space of time and when large numbers of false identities in criminal schemes have been linked to single IP addresses. Similar scalability effects as a result of digitalisation can also be seen in areas such as recruitment of young people for crime, contacts with drug consumers, cyberattacks and online fraud.

<sup>26</sup> For example, DAC2/CRS/FATCA, i.e. the automatic exchange of information about financial accounts that takes place between tax administrations. In 2023, the Swedish Tax Agency received automatic information about almost 2 200 000 foreign accounts that were thought to belong to individuals and companies with links to Sweden. Sweden shares information about approximately the same number of accounts as we receive information about.

## Insufficient information sharing between government agencies

Shared responsibility for databases and divergent missions sometimes mean that information is not shared between government agencies to the extent that is needed to better support the agencies' control activities. The resources for carrying out checks are not always sufficient given the scale of the problem. Insufficient information sharing in combination with trust between government agencies means that incorrect information has far-reaching effects at other agencies too. The incorrect information then spreads to more databases. Incorrect information in databases as a door opener to crime was raised in the 2023 Cross-agency Situation Report as one of the most serious vulnerabilities.

## The international dimension

Organised crime groups also continue to exploit the fact that government agencies are limited to the national level, and checks and databases are rarely international. The lack of information exchange is used for smuggling and criminal schemes in international trade to conceal crime proceeds and launder money, as well as to evade justice. In our globalised and digitalised society, it is possible to steer criminal activity from a distance. When criminals reside in countries that do not have extradition agreements with the EU, this makes it more difficult to prosecute the criminal activity. The lack of checks within the context of the freedom of movement for people in the EU and the single market for goods and services is still exploited by organised crime groups.

## Process-based societal systems slow down change

Government agencies and societal systems are essentially process-based and build on transparency, justice and equity. Changes and adaptations to new conditions therefore take time, as there are numerous aspects to consider. Organised crime groups, on the other hand, are situation-driven and demonstrate great and swift adaptability to new or changed circumstances. This applies to both their ability to exploit new rules and payment systems, and their use of new technology in criminal schemes. Organised crime groups are skilled at exploiting the opportunities offered by digitalisation and greater anonymity in their criminal schemes, for example by creating false identities and then controlling them with the use of electronic IDs.

### Example

#### Information in databases as a door opener for crime

When government agencies discover that a foreign actor is working in Sweden under a false identity, the Swedish Tax Agency can de-register that person as a false identity, as having emigrated or as having disappeared. However, information about money earned by that person remains in the database as pensionable income. This scenario opens up possibilities for the foreign actor to apply at a later stage for a Swedish pension from an EU or EEA country, for example, and the Swedish Pensions Agency is not aware that the identity is false as the identity is still in their database. Pension payments continue for the rest of the person's life, and seeing as a false identity<sup>27</sup> never ceases, this means that large sums can be extracted from the welfare systems.

<sup>27</sup> Does not apply to confirmed false identities that have been de-registered.

# Resilience and decisive action

There is broad political consensus on repressive law enforcement when it comes to organised crime groups, which is in line with society moving from a trust-based societal contract to a more controlled system. One example that exemplifies this shift from trust to control is that more and more government agencies have a law enforcement mission, and municipalities have a crime prevention mission. Another example is the establishment of the Swedish Payments Agency, which has the task of detecting, pre-empting and preventing incorrect payments from the welfare systems. Perhaps the clearest manifestation of the shift from a trust-based system is the Government's national strategy against organised crime – Resilience and decisive action – which was published in early 2024.

The national strategy is built around five overarching objectives with associated sub-targets:

## 1. Stopping criminal careers

Work on this objective involves:

- stopping young people being socialised and recruited into crime
- increasing prosecution of serious offences in criminal circles
- improving society's protection and reducing the risk of re-offending

## 2. Reducing the supply of illegal firearms and explosives

Work on this objective involves:

- more effective efforts to avert illegal importation and smuggling
- increasing the risk of detection and prosecution for offences linked to illegal firearms and explosives
- stricter control and oversight concerning the handling of and trade in firearms and explosives

## 3. Destroying the criminal economy

Work on this objective involves:

- averting the exploitation of public funds
- preventing companies and other legal persons from being used for criminal purposes
- fighting drug-related crime
- increasing the recovery of the proceeds of crime
- exploiting the potential in administrative measures

## 4. Building robustness against unlawful and undue influence

Work on this objective involves:

- safeguarding the integrity of public decision-making
- preventing threats from the inside in the form of insiders and infiltrators

## 5. Safeguarding systems for reliable identification and an efficient provision of information

Work on this objective involves:

- creating a more coherent system for identity administration with greater use of biometrics
- improving possibilities to collect, store, exchange and in other ways process information
- improving access to information in digital environments
- increasing the use of technical aids

This strategy expresses an ambition to place greater emphasis on obtaining redress for the victim, protecting society and control functions, and combating crime effectively. The strategy covers a number of legislative proposals that have entered into force or will enter into force over the next 2–3 years in order to give government agencies more proactive law enforcement tools and reduce identified vulnerabilities.

The national strategy addresses the vulnerabilities that both this Cross-agency Situation Report and previous ones have identified. The objectives in the Government's strategy include proposals and measures to destroy crime infrastructure used by organised crime groups. The objective of reducing access to illegal firearms and explosives is intended to impact organised crime groups' use of violence and intimidation. The objective of destroying criminal finances affects organised crime groups' exploitation of legal business structures and money laundering. The objective of safeguarding systems for reliable identification and efficient information provision impacts organised crime groups' exploitation of identities and fake documents. The objective of building robustness against unlawful and undue influence impacts organised crime groups' use of corruption and unlawful influence.







# Shifting effects

The material gathered and analysed for the 2025 Cross-agency Situation Report shows that the agencies' measures have an effect on crime, both in terms of how crimes are carried out and in terms of how criminals seek to evade justice. Organised crime groups will therefore adapt to the new conditions resulting from the measures included in the national strategy against organised crime. Although the national strategy against organised crime extends beyond the 2–3-year assessment horizon of the Cross-agency Situation Report, the following shifting effects are expected to be seen in organised crime.

## Shift towards other forms of association

Several of the measures in the national strategy target the use of legal business structures rather than money laundering. This will probably result in crime shifting more towards other forms of association, such as foundations or non-profit organisations.

## Crime shifting between countries

It is already the case that some Swedish criminals reside abroad so as to evade prosecution. As law enforcement cooperation at EU level has developed, there has been a certain shift to countries outside the EU, primarily countries without extradition treaties with Sweden or the EU. When the Swedish Police strengthens its cooperation with the countries where Swedish criminals are residing, the shift will probably continue and criminals will move to other countries. As a result of greater checks of businesses in Sweden, one probable shifting effect will be the increased use of businesses and accounts in other countries that do not have the same level of checks.

Sweden is affected by measures against crime carried out in other countries. For example, construction companies that are excluded from public procurement processes in Finland become active in Sweden instead.

## Shift towards increased use of bogus documents and identities

Greater possibilities for information exchange between government agencies will probably lead to the increased use of false documents and identities so that criminal schemes based on payments from welfare systems can continue, or so that criminal actors can avoid detection in government agencies' control and oversight activities.

To ensure that the provisions on confiscation are clear, easy to apply and adapted to future challenges, the Government has drawn up new confiscation legislation that entered into force on 8 November 2024. The new form of confiscation, independent confiscation, means in short that property such as cars, cash or watches can be taken from an individual who lacks the financial means to acquire such property legally – known as unexplained assets.

Government agencies are putting a great deal of effort into adapting to the new confiscation legislation. IT systems are being adapted, training courses held, new staff recruited and more. Although many government agencies have prepared with training measures, it will take time for the full effect of the new legislation to be achieved. However, in 2–3 years' time, the new legislation will probably still mean some shifting effects among organised crime groups. As independent confiscation will mean that it is important to be able to explain that assets and income are legal, the use of false documents and identities will probably increase. Another probable effect of the legislation will be that criminal actors will conceal crime proceeds better, which will make it more difficult for law enforcement agencies to trace them.



