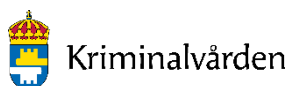


Cross-agency situation report

Organised crime 2023



Cross-agency situation report, June 2023



Published by: Swedish Police Authority, National Operations Department, 106 75 Stockholm
Ref. no: A215.519/2023, Case no: 492
Cover photo: Swedish Police Authority
Edition:

Contents

Overall assessment.....	4
1 Focus of the cross-agency initiative.....	6
1.1 What does the situation report cover?.....	7
1.2 Sources and terms	7
2 Situation report 2023.....	9
2.1 The identified threats with the greatest impact on the initiative and society	10
2.1.1 Clearer elements of economic crime in sophisticated criminal schemes.....	10
2.1.2 Criminal influence on local communities	13
2.1.3 The criminal arena is global.....	14
2.1.4 Unlawful influence	15
2.2 Identified vulnerabilities that are exploited by organised crime...	17
2.2.1 Incorrect information in databases as a door opener for crime	18
2.2.2 The cross-border criminal arena is both physical and digital	20
3 Conclusions	22
3.1 Globalisation.....	22
3.2 Welfare crime	23
3.3 Geographical expansion and violence	23
3.4 Unlawful influence	24
4 Looking ahead: threats and vulnerabilities over a 2–3-year period.....	25
4.1 Organised crime actors becoming increasingly sophisticated opponents who see Sweden as a natural choice.....	25
4.2 Effects of recession on crime.....	26
4.3 Security situation	26
4.4 Technology	27

Overall assessment

This cross-agency situation report has identified the threats that have the greatest impact on the cross-agency initiative against organised crime and on society. These are:

- economic crime as an increasingly important aspect in organised crime;
- the geographical spread of organised crime and its impact on local communities;
- the global criminal arena; and
- unlawful influence.

The most serious vulnerabilities that have been identified are incorrect data in official records being used as door openers for crime, and the physical and digital nature of the cross-border arena.

Digitalisation has meant that organised crime actors have been able to avoid being traced and this enables them to engage in and direct criminal activities from afar. The use of tools such as cryptocurrencies, neobanks and encrypted applications to launder money, transfer crime proceeds and communicate enables criminal activities to remain under the radar more than before with the help of digital developments. Increased digitalisation and public authorities' trust-based payments have resulted in a greater market for criminal services. More criminals are considered likely to have the possibility of creating increasingly advanced criminal schemes.

The use of forged, manipulated or untrue documents and certificates that are currently registered with Swedish public authorities for criminal purposes is widespread. This affects both public welfare systems and private actors.

More criminal entrepreneurs are seeking new markets outside the large metropolitan areas. This development also highlights the importance of maintaining the capability to combat the growth of organised crime in smaller places too where the presence of public authorities and resources is more limited than in the large metropolitan areas.

Developments in terms of threats and vulnerabilities over a 2–3-year period are influenced by:

- organised crime actors becoming increasingly sophisticated opponents who regard Sweden to be a natural choice for organised crime;
- the impact of recession on crime, with organised crime actors out-competing legal actors;

- the changing security policy situation in which Sweden has become more vulnerable to external security threats such as influence campaigns; and
- digitalisation leading to greater internet use combined with a steady flow of new digital financial instruments and investment opportunities that create a global market for sophisticated investment fraud.

1 Focus of the cross-agency initiative

Since 2009, twelve government agencies have been collaborating within the cross-agency initiative against organised crime. These government agencies are represented in regional intelligence centres and in the National Intelligence Service¹, which is responsible for producing a cross-agency situation report every other year. This is done on behalf of the Collaboration Council, which leads the cross-agency initiative against organised crime. Another nine agencies joined the initiative in 2018.²

Cross-agency intelligence work to combat organised crime is to focus on strategic individuals, vulnerable areas and actor- or phenomenon-based organised crime of a serious or extensive nature. In particular, the agencies are to harness opportunities to support all of society's measures to combat violent extremism, terrorism, money laundering and welfare crime.³

The task of the project group is to describe:

- changes and new phenomena since the last situation report;
- critical assets in society that are regarded as key;
- the most serious threats from organised crime;
- the most serious vulnerabilities that are exploited by organised crime;
- relevant international elements in organised crime;
- likely developments in terms of threats and vulnerabilities over a 2–3-year period, in particular international developments; and
- problems in vulnerable areas from a cross-agency perspective.

¹ The agencies involved in the initiative are 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 Tax Agency, the Swedish Security Service, the Swedish Police Authority, Swedish Customs and the Swedish Prosecution Authority. These agencies work together in the National Intelligence Centre and in seven regional intelligence centres. The Swedish Prosecution Authority only participates in regional cooperation councils and the management group of the National Intelligence Centre.

² The ten government agencies that are currently known as 'network agencies' are: the Swedish Work Environment Authority, the Swedish Companies Registration Office, the Swedish Board of Student Finance, the Swedish Financial Supervisory Authority, the Health and Social Care Inspectorate, Lantmäteriet (the national land survey), the Stockholm County Administrative Board (which coordinates the other county administrative boards in the initiative), the Swedish Pensions Agency, the National Board of Institutional Care and the Swedish Transport Agency. The network agencies do not participate in the initiative's decision forum.

³ Swedish Police Authority. *Policy document for government agencies in collaboration against organised crime*. 29.03.2022.

1.1 What does the situation report cover?

This situation report uses the same definition of organised crime as earlier situation reports.⁴ It is a broad definition that essentially does not exclude any types of crime. The situation report only covers the areas of crime that the initiative encounters, such as tax offences and fraud.

The criminal actors covered by this definition are not a homogeneous group; they include both hierarchical and loosely composed networks, distinctive groups such as motorcycle gangs, and also individuals with specialist skills and who do not have any particular allegiance but who are crucial for increased criminal capabilities.

The 2021 cross-agency situation report mentioned the five critical assets⁵ that are primarily affected by crime. This report maintains the assessment that the same critical assets are under threat and they will therefore not be the subject of further discussion in this situation report.

As is clear from the above, a cross-agency picture of the problems in vulnerable areas is included in the situation report. Section 2.1.1 only provides a short overview of this as a new report on vulnerable areas from the Intelligence Division at the National Operations Department is expected later in the year. A new project between the National Intelligence Centre and the regional intelligence centre in Police Region Mitt has been initiated and intelligence gathering is under way.

1.2 Sources and terms

To more easily identify deviations, the point of departure for the gathering of documentation has been the same coverage areas as for the 2021 cross-agency situation report.⁶ To identify changes and new phenomena, documentation has also been collected from the collaborating agencies at the National Intelligence Centre and the regional intelligence centres, as well as from open sources. In addition to this, documentation has been collected from the Swedish National Council for Crime Prevention, the Psychological Defence Agency and Region Stockholm.

⁴ 'Organised crime' refers to 1) at least two individuals who 2) over time 3) cooperate to commit serious crime 4) for the purpose of financial gain.

⁵ Security, safety and health; vital societal functions; democracy and the rule of law; Sweden's freedom, security and sovereignty; stability and security in the region; maintaining and strengthening EU cooperation and integration; promoting a multilateral world order. Prime Minister's Office. *National Security Strategy*. 2017.

⁶ Swedish Police Authority, National Intelligence Centre. *Cross-agency situation report. Organised Crime 2021*.

Applying a broad definition of the term ‘organised crime’ means that the situation report can only provide a general assessment of threats and vulnerabilities on the basis of the agencies’ shared and individual missions, and the intentions, capabilities and room for manoeuvre of criminal actors. The situation report uses these three terms as a point of departure for identifying the most serious threats and vulnerabilities.

‘Intention’ refers to the relationship between criminal actors’ ambitions, motivation and desire or need for profit, power, freedom or protection. ‘Intent’ refers to future intentions and prospects.

‘Capability’ refers to a threat actor’s capability or real potential to achieve their intention or their desired results based on their skills and resources and potential in the right circumstances. Examples of capabilities are organisation, skills, equipment and resources.

‘Room for manoeuvre’ involves an actor’s possibilities and restrictions in terms of committing offences. Examples are legal and administrative regulations, ongoing conflicts or access to criminal markets.

These terms can also be used to describe public authorities’ own or joint intentions, capabilities and room for manoeuvre to reduce threats and vulnerabilities emanating from organised crime.

As a rule, the intention is included in public authorities’ mission, policy documents and strategic objectives.

Capabilities can be assessed on the basis of staff resources, skills level and technical equipment, for example.

Room for manoeuvre is primarily dictated by legislation, mission, priorities and the balance between control, service and efficiency.

Using the same terms helps us to identify the areas in which the gap between the overall criminal threat and public authorities’ possibilities to reduce this threat is the greatest.

2 Situation report 2023

To be able to compare changes since the last situation report, here is a summary.

Identified threats 2021	Change 2023
Attacks on the welfare system and the evasion of taxes and charges	Clear attacks, also on regions and municipalities
Drugs crime and the serious violence resulting from it	Escalated spiral of violence with lethal firearm violence and explosions, also outside the large metropolitan areas
Parallel societal structures that challenge the rule of law	Indications of geographical spread of organised crime
Identified vulnerabilities 2021	Change 2023
Anonymity in the legal sphere of society	Still a relevant vulnerability
Trust-based systems in combination with inadequate control mechanisms	Still a relevant vulnerability
Public authorities' shared responsibility gives rise to loopholes	Still a relevant vulnerability
Corruption, infiltration and unlawful pressure in the legal sphere of society	Scope not clear but clearer intention and capabilities of certain actors
National law enforcement in the area of cross-border crime	Clearer that organised crime is partly governed from abroad

Figure 1. Table of changes to identified threats and vulnerabilities since 2021

In the 2021 situation report, the most serious threats were considered to be attacks on the welfare system and crime in the form of the evasion of taxes and charges, drugs crime and the serious violence resulting from it, and the emergence of parallel societal structures. The most serious vulnerabilities that were exploited were divided into five categories: anonymity in the legal sphere of society; public authorities' trust-based systems in combination with inadequate control mechanisms; public authorities' shared responsibility; corruption, infiltration and unlawful pressure in the legal sphere of society; and national law enforcement in the area of cross-border crime.

The threats and vulnerabilities described in the 2021 situation report are still considered relevant for the cross-agency initiative against organised crime to try to reduce in future as well. The threats and vulnerabilities raised in the 2023 situation report are not new phenomena; rather, they should be seen as clarifications based on new insights achieved from ongoing work in the field.

To implement the recommendations submitted in the 2021 situation report, work is under way concerning bureaux de change, company mediators, a cross-agency strategy for vulnerable areas and a reinforcement of the analytical capability of the cross-agency initiative against organised crime. The Intelligence Division at the National Operations Department has drawn up the report *Crime proceeds as a larger societal problem*, based on information from the Swedish Police Authority, the Swedish Tax Agency, the Swedish Social Insurance Agency, the Swedish Public Employment Service and the Swedish Enforcement Authority.

2.1 The identified threats with the greatest impact on the initiative and society

Within the context of organised crime, all manner of offences are committed, ranging from unlawful appropriation to sophisticated economic crime with complex elements that reach far beyond Sweden's borders. The level of organisation in organised crime has increased through sophisticated and multi-criminal crime schemes. Over time, cross-border crime has expanded to encompass a global and digital arena.

In recent years, increased awareness within the cross-agency initiative against organised crime has identified two economic crime phenomena that are probably a threat to the functioning of society. One is attacks by criminal networks against the welfare system. The other is the fact that more people are becoming involved in the legal sphere of society in order to broaden their criminal activities.

Below are the most serious threats that the National Intelligence Centre considers to have the greatest impact on the initiative and on society as a whole. These are:

- economic crime as an increasingly important aspect in organised crime;
- the geographical spread of organised crime and its impact on local communities⁷;
- the global criminal arena; and
- unlawful influence.

2.1.1 Clearer elements of economic crime in sophisticated criminal schemes

Economic crime has become an increasingly important part of organised crime. Several regional intelligence centres note that criminal actors are gaining more knowledge when it comes to criminal schemes that use business operations as crime instruments in the form of companies, associations and foundations. Companies are predominantly based in Sweden, but in recent years it has become increasingly common for criminal actors to use foreign companies as crime instruments.

Economic crime covers a whole host of different criminal activities, from simple fraud to sophisticated criminal schemes that often combine legal and illegal transactions. The combination of legal and illegal activities makes

⁷ This refers to small and medium-sized towns.

investigations more difficult. Technical developments and digital transactions are additional challenges. A closely related term is the criminal economy, which refers to the ecosystem of crime proceeds that are generated, handled and partially reinvested in future criminal activities. It also covers legal funds that are used to invest in criminal activities. The money that flows in the system is money from illegal activities that is consumed by households or used to buy luxury goods. It is reinvested in illegal activities or it enters into the legal system in or outside Sweden, making detection and prosecution more difficult. The ‘legitimate’ money in the system enters the illegal market through various forms of welfare fraud, loans or investments, for example.

There has probably been an expansion of this kind of crime. While the state has been the main target up until now, welfare payments from municipalities and regions are now also being targeted, for example to medical clinics, residential care homes for children and young people, sheltered accommodation and foster families. There is a risk when no permits are required to set up various forms of establishments, and several challenges have been identified in the area of unscrupulous actors specialising in welfare crime⁸ against regions. This applies, among other things, to the lack of national databases, the lack of overview and of possibilities to see patterns that stretch beyond specific systems, and difficulties demonstrating the scope of an activity when there is a mixture of incorrectly and correctly conducted activities.⁹

The incorrect prescribing and use of medication¹⁰ have been identified by Region Stockholm as a major risk given that almost 10 000 doctors and dentists without a Swedish personal identity number or coordination number are entitled to prescribe medication in Sweden.¹¹ On 1 January 2023, Region Stockholm introduced new rules to get to grips with the illegitimate prescribing of medication within the pharmaceutical benefit scheme. The rules concern the requirement for private caregivers to have what is known as a ‘workplace code’.¹² However, it is not thought that this change to the rules will have any

⁸ According to the National Council for Crime Prevention, welfare crime primarily covers benefit fraud and offences against the welfare system, but it also includes support and payments to associations and organisations. If this procedure also takes place systematically over time, with the help of incorrect certificates and companies used as crime instruments, this is a matter of advanced welfare crime. See also *Advanced welfare crime – pre-emption, prevention and prosecution* (SOU 2017:37).

⁹ National Council for Crime Prevention. *Welfare crime against municipalities and regions*. Report 2022:1.

¹⁰ Including pharmaceuticals that are classified as narcotics or doping substances, as well as pharmaceuticals used for beauty purposes,

¹¹ It is not known how many of these doctors and dentists are actually practising the profession and which countries they are resident in. The authorisation that provides a prescription code is issued by the National Board of Health and Welfare.

¹² <https://www.lakemedelsvarlden.se/region-stockholm-vill-stoppa-oserios-forskrivning/>.

major effect on the types of doctors and dentists mentioned above, as the Administrative Court and the National Board of Health and Welfare have stated that Region Stockholm does not have the right to close down workplace codes.

Both Region Stockholm and Region Västra Götaland have identified links to organised crime among both caregivers and patients¹³. This problem is probably also present in other regions too. The pharmacy market also has problems in the form of unscrupulous private actors, and also limited possibilities for supervisory bodies to carry out checks.

Crime within and against businesses¹⁴ continues to be a serious problem. Companies used as crime instruments are a prerequisite for engaging in economic crime. The same assessment has been made in previous cross-agency situation reports and investigations.¹⁵

Freedom of movement in the EU makes it easier to move capital and people across national borders. This is largely because of rapid IT developments and globalisation. For example, it is relatively easy for criminal actors who commit tax offences and money laundering to conceal their assets and move them to other accounts. They are able to exploit welfare systems for criminal purposes due to factors such as globalisation and technical developments.¹⁶

The importance of enablers¹⁷ of economic crime is probably increasing given the growing overlap between organised economic crime and criminal networks. Network actors who are higher up the hierarchical chain engage in economic crime in order to distance themselves from other crime, such as drugs offences and serious violence. The activities of enablers are often not illegal, and even in other respects they can be difficult to investigate. If these illegal activities are detected, they often result in minor penalties.

A limited company is the most commonly used company form for committing economic crime. Criminal actors have increased their knowledge and understanding of how this company form can be used to commit crime. They either start a company themselves for criminal purposes or they buy up existing

¹³ Individuals who use fake certificates to claim that they are sick or have some form of disability.

¹⁴ Limited companies, trading companies, sole proprietorships, limited partnerships, foundations and associations.

¹⁵ See, for example, the cross-agency situation reports on organised crime from 2019 and 2021, and *Bolaget som brottsverktyg* (The company as a crime instrument) (ToR 2021:115).

¹⁶ <https://www.ekobrottsmyndigheten.se/internationellt-samarbete/>

¹⁷ ‘Enablers’ refers to actors with criminal or legitimate intentions who enable critical steps in a criminal scheme, such as tax advisers, exchange companies, decision-makers in public sector activities or administrators of marketplaces.

companies that in many cases have little or no turnover. They then increase turnover using incorrect annual reports in order to create a high rating on paper. However, the actual increase in turnover is questionable.

Companies are used to enable all kinds of criminal activities.¹⁸ In some cases, actors move in both criminal circles and circles with links to violent extremism. Not just limited companies but all types of company are potentially vulnerable to exploitation by organised crime. This also applies to associations where there is a lack of checks concerning principals, boards and activities.¹⁹

To a certain extent, criminal actors check company structures directly or indirectly through infiltration in order to enable their criminal activities. Criminal actors also set up dummy companies in order to use these to infiltrate the legal market.²⁰ Access to companies is now crucial and a prerequisite for most criminal schemes, and also to crime in working life. This area of crime covers a whole range of economic crime, such as money laundering, MTIC fraud schemes and excise duty crime, often in combination with exploitation of human beings and work environment offences.

2.1.2 Criminal influence on local communities

Since 2013, the proportion of cases of lethal violence had been relatively stable, but in 2022 fatal shootings – which are very much linked to vulnerable areas – were behind more than half of the total number of fatalities. Vulnerable areas continue to be a breeding ground for organised crime, but the problems identified by the Police have remained relatively stable in the past two years in the three areas on which the assessment is based.²¹ There is some concern that similar problems linked to vulnerable areas could arise outside the larger cities too. Serious and lethal violence is still occurring in large cities, but it has also become more common in medium-sized and smaller towns and especially in places that are not covered by the Swedish Police Authority's list of vulnerable areas. Another change is that younger perpetrators are committing serious violent crimes. Younger people are rarely the subject of

¹⁸ For example, the withholding of taxes and charges, erroneous payments such as allowances and benefits using false identities or straw men, and the financing of terrorism. Companies often have several criminal schemes, such as fake control statements and credit fraud, fake invoices, illegal work, wage guarantees, VAT fraud, withholding customs, withholding tax, investment fraud and CEO fraud. They are often represented by a straw man or a foreign/false identity.

¹⁹ Swedish National Audit Office. *Tillit och kontroll – statlig bidragsgivning till civilsamhället* (Trust and control – state benefits to civil society) RiR 2023:7.

²⁰ Europol. *The Law Enforcement perspective in the wake of the Pandora Papers Leak*. December 2021.

²¹ Living environment and safety, societal systems and social development/effects.

government agency measures within the cross-agency initiative against organised crime, and early measures on the part of other societal actors²² may therefore have a better crime prevention effect.

There are indications that local networks have become established in a larger geographical area and have become regional, and in some cases national – for example with regard to crime linked to family-based criminal clans and drug networks. Another cause is the lack of government agency presence which can make it more difficult to carry out checks of businesses, which in turn can offer greater opportunities to engage in criminal activities.

It has also become clear that conflicts are spread from abroad to Sweden by Swedish criminals, which can aggravate existing problems at local level. There is also the opposite phenomenon, with conflicts being transferred from Sweden to abroad.

Criminal actors can have a major negative impact on local communities. Sometimes property is bought to be used for criminal purposes, such as storage or manufacture of illegal goods. There have also been cases of locally based criminal actors with links to larger cities or who engage in smuggling from abroad.

2.1.3 The crime arena is global

Developments in the area of ‘fintech’²³ offer new possibilities for criminal actors to move assets, launder money and evade tax. Neobanks²⁴ and cryptocurrencies are examples of global financial systems and they provide parallel economic structures that circumvent money laundering checks and public oversight as they have few points of measurement in relation to the rest of the economic system. Transfers take place immediately and are difficult to trace.²⁵

Despite technological developments, cash is still very much used. Money remittances such as hawala²⁶ make it difficult to follow the transfers. There is a risk that these transfers are for the purpose of money laundering or financing of terrorism, or even tax evasion.

²² Such as schools and social services.

²³ Financial technology that combines financial services with software technology.

²⁴ A neobank can most simply be described as a digital bank where the user can perform all services using a mobile app or a web interface.

²⁵ Swedish Police Authority. *The Financial Intelligence Unit Annual Report 2021*. April 2022.

²⁶ Hawala is Arabic for ‘transfer’ and in short means that a financial service is conducted outside an established financial system.

The global crime arena also includes the digital domain where all parts of Swedish society are potential targets for cyber attacks. The threat actors can be divided into state actors (foreign powers), criminal actors, ideologically motivated actors and lone actors. The global increase in cyber crime is largely due to the fact that there has been growth in the criminal market offering tools and services for committing cyber crime. As the business of ‘criminal schemes for sale’ is international, there are good opportunities for expanding activities by committing more fraudulent acts or cyber-related crime.

Another way of giving a façade of legitimacy to criminal activities is to use Swedish companies in international criminal schemes. It is easy to register companies, and open business registers create credibility, but the information has not always been verified. For example, Swedish banks and customs declarations can give legitimacy to international crime.

Criminal actors are constantly developing their methods through more long-term planning and more professional criminal schemes, which in turn leads to more international activity. This makes crime more difficult to detect and investigate. Countries outside the EU, such as Morocco, Türkiye, the United Arab Emirates and Thailand, are increasingly used as logistical and financial hubs.

The cross-border spread of organised crime increases the risk of involvement from foreign powers that use criminal actors to promote their own interests. For example, Russian-speaking organised crime has been pointed out as a foreign policy tool that can be exploited in intelligence contexts and to exert political and economic influence. The geographical expansion of crime and the use of strawmen are probably not limited to foreign criminal actors that are directing crime in Sweden; this probably includes state-sponsored crime too.²⁷ Other examples of other states’ interests meeting organised crime based in Sweden are when members of a known family-based criminal network met a foreign ambassador in connection with an influence campaign against Swedish social services, or Türkiye’s refusal to extradite a leading criminal actor.

2.1.4 Unlawful influence

Organised crime is extensive, multi-criminal and multifaceted. It poses a threat to our democratic society. One of the most serious components of this threat picture is when staff of municipal and state administration, political

²⁷ Examples of state-sponsored crime can be weapons smuggling, violation of sanctions, immigration fraud, exploitation of human beings, influence campaigns, acting as a strawman for the purchase of tactical assets or assets of strategic interest (such as properties close to facilities with protected status) or the purchase of services for cyber attacks.

bodies at local and national level, and private businesses are subjected to unlawful influence.

Unlawful influence is used in the situation report as an umbrella term for various criminal and non-criminal approaches aimed at influencing political decision-making, freedom of expression and the judicial process, and directly or indirectly influencing the exercise of public authority and decision-makers in the business sector. Closely linked to criminal acts is unlawful influence in the form of disinformation campaigns. This term also covers infiltration which, in itself, is not criminal but which is aimed at directly or indirectly influencing the exercise of public authority for criminal purposes.

Unlawful influence can be seen as a pyramid comprising various steps that reflect criminal actors' intentions, capabilities and room for manoeuvre.

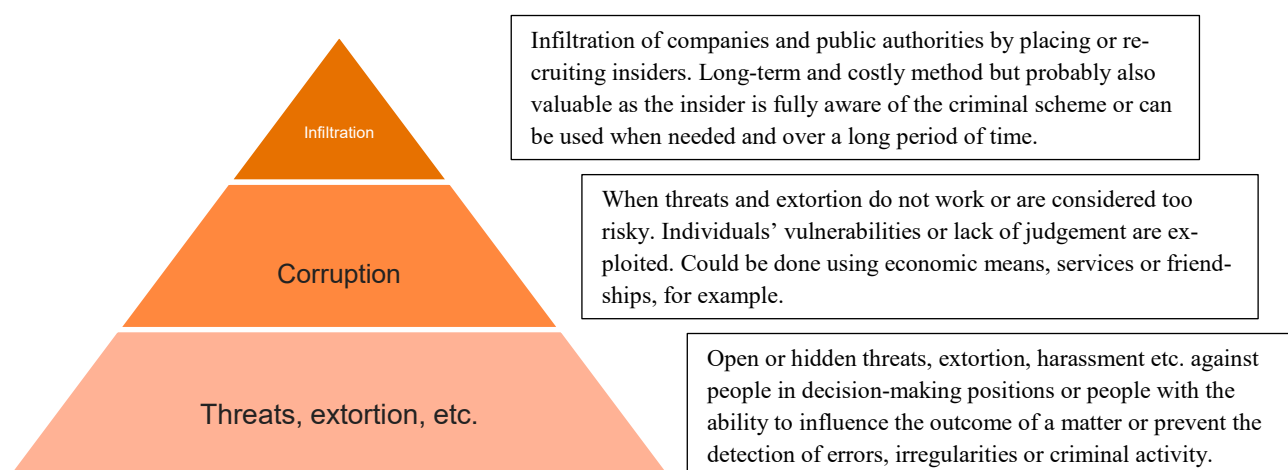


Figure 2. Illustration of various forms of unlawful influence. The higher up the pyramid, the more resource-intensive and long-term a strategy is required.

Through their use of unlawful influence and infiltration, organised crime networks and actors have probably won even greater power and influence. The use of corruption and the exploitation of legal company structures are among the key factors for organised crime, and they appear in everything from small-scale bribes to advanced economic criminal schemes.

In many regions, criminal networks' capabilities have become clearer when it comes to the exploitation of insiders in legal activities, such as banks, public authorities and lending institutions. The healthcare sector is also affected. The fact that criminal networks engage in systematic extortion in the form of punishment and protection rackets targeting individuals and companies is another reason for this increase. The actors include both family-based criminal networks and motorcycle gangs.

Shortcomings have also been identified in municipal administration, for example in cases where people have approved each other's invoices or in cases with far-reaching problems concerning incorrect planning permission.

One possible consequence of unlawful influence could be the emergence of a culture of silence. This can manifest itself in different ways, such as certain phenomena not being reported, managers not supporting their staff, or employees feeling that certain norms in society have been set aside.²⁸

Unlawful influence has also occurred as part of subversive activities²⁹, such as the campaign targeting social services at a higher level that aimed to undermine confidence in Sweden and Swedish authorities. Parts of this campaign, which has included death threats against social services staff, have been directed from abroad and have also had links to family-based criminal networks in Sweden. Not only does this type of activity risk undermining confidence in important societal functions, it also risks increasing the polarisation of society, which in turn fuels extremism and contributes to a heightened threat picture.

Another aspect of unlawful influence is concern among many public authorities that activities conducted in smaller towns or rural areas risk being subjected to attempts to exert unlawful influence, for example when recruiting staff or because of new tasks due to rapid developments in society and political decisions.³⁰ As consideration must be given to both employment law and security, the functions that may be affected include HR, intelligence and security, as well as internal investigations into the sharing of information about individuals and their relationships.

2.2 Identified vulnerabilities that are exploited by organised crime

Criminal schemes and the growth of organised crime are essentially enabled by loopholes in legislation and vulnerabilities in society. These are exploited by organised crime actors. The description of threats above identifies a

²⁸ Anna Ekström. *Finns det en tystnadskultur i Göteborg stad? (Is there a culture of silence at Gothenburg Municipality?)* 26.08.2021.

²⁹ 'Subversive activities' means the kind of security threats that are aimed at covertly bringing down or changing the democratic form of government or placing the country in a position of dependency in relation to a foreign power, and that are achieved through methods such as propaganda, disinformation, infiltration, crime, sabotage and terror threats (see the Swedish Security Service Yearbook 2022-2023).

³⁰ Various forms of support in connection with the COVID-19 pandemic and high electricity prices.

number of vulnerabilities that feature in many criminal schemes. The vulnerabilities identified in the last situation report are probably still relevant. A number of legislative inquiries³¹ are under way to close the loopholes exploited by organised crime actors. However, organised crime is a complex activity and actors are continuously identifying loopholes to evade detection and prosecution. Reducing vulnerabilities is therefore a long process. This section describes the vulnerabilities identified. They have been identified in the threat assessment as being recurrent within the context of the most serious threats.

The most serious vulnerabilities identified are:

- incorrect information in databases as a door opener for crime; and
- the cross-border arena that is both physical and digital.

2.2.1 Incorrect information in databases as a door opener for crime

More and more public authorities are expanding their digital services in order to make contact with citizens easier. Rapid digitalisation with electronic ID and information provision makes things straightforward and efficient for the majority, but it also creates space for criminal groups to freely use fake, manipulated and incorrect certificates or documents as part of their criminal activities. In some cases, this is done systematically and on a large scale, which can cause a great deal of harm. More thorough checks of the information provided and then registered are only carried out as an exception and often on formal grounds. Risk-based automated selections for checks are rarely permitted.

All public authorities have their own mission, but there are sometimes overlaps. This can create uncertainty over which authority is responsible or where the primary responsibility for oversight lies. This can result in an inadequate overall picture and a risk of lacking accountability.

Swedish society and Sweden's public authorities are essentially based on a system of trust, with the information in databases having been provided by individuals and companies. An error with the first authority can have a major impact if databases are not compared to identify deviations. Many recipients that maintain databases also lack the mission or mandate to assess the reliability of the information received. The information registered with public authorities is therefore rarely or never scrutinised with a critical eye.

³¹ Examples include *The responsibility of municipalities for crime prevention work* (ToR 2019:94) and *Tougher penalties for crimes in criminal networks* (Gov. Bill 2022/23:53).

Criminal actors and groups have the intention and capability themselves or via enablers to exploit the trust-based system, as is the case with crimes against the welfare system, for example. There is a great deal of room for manoeuvre as fake and incorrect information can be provided digitally and often anonymously.³²

The intention of public authorities that maintain databases when it comes to combating breaches of regulations and preventing crime can vary. If an authority does not have a law enforcement mission, the level of intention may be considered to be low, which may also have a negative impact on capabilities and room for manoeuvre. Capabilities may be limited by staff resources, lack of knowledge about the problem, technical tools and more. The biggest risks in terms of limiting competent authorities' room for manoeuvre are that there is a lack of support in the legislation or the mandate for more thorough checks, the geographical coverage is so large, and there is an imbalance between service and checks, for example.

In view of crime trends in recent years and the existing security policy climate, the importance of the reliability of the information contained in public authorities' databases should not be underestimated. Incorrect information in databases is a common crime instrument for profit-driven crime, but providing incorrect information can also have an underlying motive, such as unlawful influence and threats to the system in order to destabilise important societal functions.

Fact box: The Swedish Population Register: a door opener to crime. Fraudulent registrations in the Swedish Population Register are reported to have become increasingly common, which is also indicated by the fact that there has been an increase in reports to the Police. It is therefore worrying that there are probably many cases that go unreported, despite public authorities' responsibility under the Swedish Population Register Act. The Swedish Tax Agency and the cross-agency initiative against organised crime already have indications that there are probably at least 200 000 individuals in Sweden who are registered incorrectly. Incorrect registrations are common in the building, restaurant, cleaning and removal sectors, where people without a residence permit are often subjected to wage exploitation in unqualified and sometimes risky professions.

It has also been noted that criminals seek to protect their personal data to a greater extent to make it more difficult for public authorities to identify them. Another tactic is to change one's name to a common name.

³² By exploiting identities, strawmen or dummies.

2.2.2 The cross-border criminal arena that is both physical and digital

Organised crime has probably become more complex insofar as more criminal actors and networks are engaging in economic crime. These actors are also operating in an international arena – from other countries and also in the digital sphere. The 2021 cross-agency situation report against organised crime highlighted cross-border crime with national crime prevention as a vulnerability. The same vulnerability remains in this year's situation report.

This complexity is possible because control mechanisms and legislation are still national and are probably not designed to address cross-border crime.

Large volumes of import and export goods provide many smuggling opportunities for organised crime actors. An ever faster flow of goods has arisen as a result of society's demand for efficient transport. This makes it more difficult for public authorities to check goods to ensure that the contents are correct and that restrictions and sanctions are being followed. Public authorities' routines and control resources are also mapped out by criminal actors, for example through counter-surveillance and distraction tactics.

The criminal sphere can be described as individuals with a large network of criminal contacts who have specialist skills. It can also include access to key functions in the smuggling scheme, such as ports, companies, logistics, criminal schemes, transport and bribed officials or staff. Ports have been identified as a vulnerability as maritime transport is exploited for the large-scale smuggling of illegal goods into Sweden. It is important to also establish what the ownership situation is, as ports are part of Sweden's critical infrastructure.

Specialists may belong to a specific network or they may also work on behalf of others. Skills and contacts regarding specific criminal schemes are spread in the criminal sphere. Smuggling is organised not only to Sweden but wherever there is an opportunity for financial gain.

Despite the lion's share of the current economy being digital, there is widespread use of cash and a parallel financial market for cash in Sweden. Money remittance services and bureaux de change are the cornerstones of the parallel economy, where crime proceeds are mixed with legitimate money. Examples of sectors that are cash-intensive include trade in work permits, the building sector or various forms of seasonal work where employers do not pay any social security contributions. Large volumes of cash are placed in manual deposit machines all around Sweden. A large proportion of these deposits are carried out by money remittance services, thus enabling criminals to launder money. Each year, billions of Swedish kronor are flown back into

Sweden. This money is probably partly made up of crime proceeds³³ that are reinvested or invested abroad as part of money laundering. One challenge in this context is establishing the origins of money coming in from abroad, as this is probably ‘laundered’ money.

The digitalisation of society has made it easy for people to quickly access services. Yet this also creates a distance to public authorities as visits in person are no longer necessary for purposes of identification. As noted in the 2021 situation report, the electronic identification system³⁴ is a door opener for criminal actors. A criminal actor who has at their disposal a large number of electronic IDs with the associated accounts can easily and with a relatively low level of risk commit crimes in the exploited identity’s name, then moving crime proceeds between other exploited identities. This procedure poses major challenges in terms of the burden of proof in criminal investigations.

Fact box: Logging in to banks using an electronic identification is a security risk. Telephone fraudsters use what is known as ‘telephone phishing’ to trick people into logging in to their online bank and, in doing so, unwittingly approving large bank transactions. Electronic identification for mobile phone use is a very popular tool among criminal entrepreneurs specialising in immigration fraud and creating fake identities or hijacking others’ identities. Access to and control of an electronic identification, together with a personal identity number, means that fraudsters can control a large number of identities with the associated accounts without even needing to be present in the country.

One aspect of digitalisation is the growth of fintech companies, such as neobanks³⁵. Neobanks are only obliged to report in the country in which they are registered, which can mean a great deal of risk from a money laundering and terrorism financing perspective. Neobanks represent a vulnerability as it is possible to maintain a parallel economy that is hidden from one’s own traditional bank and from law enforcement agencies.³⁶ Banks’ 360-degree

³³ They are also made up of halawa transactions that are sometimes remittances and legitimate transfers but sometimes cash generated by illegal work.

³⁴ In 2019, approximately 8.5 million inhabitants had an electronic ID, of which approximately 7.8 million had an electronic ID for use on mobile phones. More than 600 websites support electronic identification. Only people with a Swedish identity number can obtain an electronic identification. Electronic identification is used for the services of most public authorities, regions, banks and a number of other services in society, not least payment services.

³⁵ An online database lists 246 neobanks globally, of which 76 are in Europe and 19 in Sweden. Neobanks are entirely digital and can have cross-border operations, meaning that their customer base may also be outside the country in which the banks are registered.

³⁶ Swedish Police Authority (Financial Intelligence Unit). *Neobanks. A report on neobanks and their risks related to money laundering and financing of terrorism*. May 2022.

perspective and knowledge of customers becomes more difficult when individuals have several banks, both Swedish banks and neobanks.

3 Conclusions

Since the 2021 situation report, a number of changes have been identified in criminal schemes. The increase in criminals' capabilities in recent years is largely due to society's conditions for reducing threats and vulnerabilities.

3.1 Globalisation

Sophisticated criminal schemes are not limited to Sweden; they are spread across several countries and various jurisdictions, for the purpose of evading detection and prosecution. It is therefore not sufficient to prevent and combat organised crime locally, regionally and nationally. Digitalisation has led to criminal networks and actors avoiding being traced by using tools such as cryptocurrencies, neobanks and encrypted applications in order to launder money, transfer crime proceeds and communicate. Another consequence of digitalisation is that there are now greater possibilities to engage in and direct criminal activities from a distance.

When criminal actors do enter the legal sphere, the crime prevention tools are not enough, especially not for combating international schemes when legislation is national. For crime prevention measures to be successful, more international collaboration is needed than is currently the case, for example within Impact³⁷ or with Interpol.

Based on the criminal scheme in question, relevant parties are involved to commit the crime. The inner circle often comprises just a few individuals and relations are largely based on trust. Leading figures often distance themselves from activities by not having any close contact with the people who carry out the crimes. Increased digitalisation and public authorities' trust-based payments have resulted in a greater market for criminal services. More criminals are considered likely to have the possibility to commit increasingly advanced criminal schemes.

Greater communication opportunities with mobile chat functions and fewer border controls, for example, also provide greater opportunities for criminal actors to control crime carried out in Sweden from other countries. This

³⁷ Impact, European Multidisciplinary Platform Against Criminal Threats, is a form of collaboration adopted by the European Union in 2010 with the aim of jointly working to combat the most serious types of crime and threats against the EU.

could be everything from the planning of drugs crime or fraud to instigating serious violence and involvement in local and national conflict environments.

3.2 Welfare crime

Crime against the welfare system results in tax-financed benefits ending up in the hands of criminals, which in turn leads to trust in the social contract being threatened. Crime in working life leads to people being exploited, tax revenue being withheld and incorrect payments being made, as well as competition in the business sector being distorted. Unscrupulous companies manipulate the regulatory system, setting aside competitive neutrality.

The definition of crime against the welfare system should be broadened to include more societal actors than has traditionally been the case, such as state, regional, municipal or private actors that can help to combat deliberate and systematic attacks on funds that are administered collectively, irrespective of who the injured party is. The use of forged, manipulated or untrue documents and certificates that are currently registered with Swedish public authorities for criminal purposes is widespread, both in the public welfare system and with private actors. An incorrect or false piece of information that has been registered with a government agency may form the basis of a decision or a registration with another agency, and so on. This can result in a domino effect in a short space of time with other societal actors.

3.3 Geographical expansion and violence

Access to drugs is thought to remain unchanged, despite the fact that law enforcement agencies have obtained access to encrypted material and prosecuted a large number of criminals. Criminals' hunt for crime proceeds and status have meant that there are many people willing to fill the gap. Despite positive results in terms of prison sentences and seized weapons, drugs and cash, there has only been a marginally dampening effect on organised crime in terms of intentions, capabilities and room for manoeuvre. Drugs-related conflicts resulting in lethal gun violence and explosions will therefore probably remain at the same high levels. Smaller towns with good logistical conditions for the distribution of drugs and limited police presence will probably be affected by these conflicts to a greater extent than is currently the case.

Given the relatively large number of Swedish criminals who are abroad and given the ongoing conflicts, it is likely that some of these conflicts will be transferred to other countries, resulting in serious violence.

Organised crime needs to be seen from a non-traditional angle. Where there used to be organisational, partly hierarchical structures, criminals today

operate as entrepreneurs who primarily represent themselves. There are no clear loyalties between them, and collaboration takes place pragmatically for the purpose of increasing crime proceeds. Collaboration takes place on the basis of individual specialist skills and contact networks, for example in the areas of smuggling or distribution of drugs. The actors are multi-criminal.³⁸ They move across many regions and are not geographically limited in the same way as was previously thought.

Many criminal entrepreneurs and networks are seeking new markets outside the large metropolitan areas. This is a development that highlights the importance of maintaining the capability to combat the growth of organised crime in smaller places too where the presence of public authorities and resources are more limited than in the large metropolitan areas. This will probably become a challenge for municipalities, not least small ones, in their future responsibility for crime prevention work.

3.4 Unlawful influence

Unlawful influence is an area with several dimensions: from individual to national and international level, from threats to infiltration, from opportunity to strategy. More advanced forms of unlawful influence will probably become more common, as well as threats and assaults committed by underage perpetrators. The complexity of the problem makes it difficult to identify delimitations and also leads to shortcomings in terms of an overall view and division of responsibility between public authorities and functions. Several actors outside the cross-agency initiative against organised crime may therefore need to be involved so as to better understand the problems and take other measures than those that are currently possible.

In the wake of a changing security policy situation, Sweden has become more vulnerable to external threats in the form of activities threatening our security, such as influence campaigns by foreign powers. At the same time, there are indications that organised crime actors are using unlawful influence to a greater extent.

With some criminal actors, there are indications of changing intentions. Behind a legal façade as an entrepreneur, for example, a criminal actor can create a network of contacts in the business sector and in politics. By infiltrating and corrupting companies, banks and public authorities, criminal actors increase their room for manoeuvre. This can give them a power base in the local community, with the associated risks of influence of democratic or administrative law processes, for example. Power ambitions for criminal

³⁸ National Council for Crime Prevention. *Drugs markets*. Report 2021:10.

purposes are difficult to detect. This is a challenge for the legislator and for public authorities that work against organised crime in general, and against infiltration and corruption in particular.

4 Looking ahead: threats and vulnerabilities over a 2–3-year period

The project group's terms of reference included describing likely developments in terms of threats and vulnerabilities over a 2–3-year period, in particular international developments. The points below should not be seen as final, as the problems can change over time.

4.1 Organised crime actors becoming increasingly sophisticated opponents who regard Sweden as a natural choice

The threat from organised crime is now more complex and multifaceted than before. Although intentions in terms of gaining profit remain unchanged, capabilities and room for manoeuvre have increased. Organised crime was previously characterised by drugs offences, violence and gross theft³⁹. Now, a whole host of other phenomena can be added to the list:

- organised and large-scale attacks on the welfare system;
- advanced international investment fraud;
- money laundering via global networks;
- unlawful influence by means of infiltration;
- criminal expansion to smaller towns;
- crime by proxy, also from abroad;
- exploitation of human beings in shadow society, often third country nationals;
- illegal waste management;
- business as a crime instrument;
- exploited identities; and
- fake documents and false information in databases.

The fact that this list has become so long suggests a lack of adaptation within the cross-agency initiative against organised crime to new, expanded crime phenomena. The lack of continual strategic analysis can be said to be a vulnerability, but above all a failure to set the right priorities among measures to address threats and vulnerabilities that had already been identified. The list

³⁹ For example bank robberies, cash in transit robberies and smash and grab thefts.

will probably grow even longer unless there is a revised view of a cross-agency mission that favours Swedish society as a whole and takes greater responsibility for preventing crime, and unless there is clearer political direction. The cross-agency initiative against organised crime should work to prevent and reduce vulnerabilities that threaten the functioning of society and provide a breeding ground for organised crime, having a negative impact on society, even in cases that do not involve actual criminal offences.

4.2 Effects of recession on crime

The difficult economic situation, with high inflation, high interest rates and recession, will probably dampen the willingness to invest and limit the market for risk sectors. One example is the construction industry, which has a key role to play in terms of the economy and an important role in organised crime. Large infrastructure projects become clear targets when other projects are slowed down or stalled.

An expected increase in unemployment will probably aggravate the situation for groups in the labour market that are already vulnerable. We can probably expect a growing shadow society in the wake of recession.

In 2022, the number of company bankruptcies rose compared with 2021. Businesses are a key asset in bankruptcy-related criminal schemes. Bankruptcy-related crime, such as bankruptcy fraud, credit fraud and the exploitation of wage guarantees, will probably increase during the recession. An increase in the number of companies experiencing financial problems will probably provide greater opportunities for organised crime actors to acquire companies for criminal purposes.

The worsening economic situation can also be expected to have an impact on market-driven crime in the large metropolitan areas, where demand for drugs, for example, can speed up the geographical expansion of organised crime to small and medium-sized towns.

4.3 Security situation

The full-scale Russian invasion of Ukraine in February 2022 and Sweden's application to join NATO have led to a changed security policy situation that makes demands in terms of awareness and greater focus, above all on Russian-speaking organised crime that is already established in Sweden. It could be a potential foreign policy tool that can be exploited in intelligence contexts and to exert political and economic influence. In light of the worsening

security situation over the past year, there is reason to expect that unlawful influence in the form of subversive activities will increase.⁴⁰

4.4 Technology

A general increase in internet use combined with a steady flow of new digital financial instruments and investment opportunities create a global market for sophisticated investment fraud. This will probably increase in the years ahead. Other forms of fraud, such as cases in which voices have been cloned using artificial intelligence (AI), have already been noted in Sweden.

Developments in the area of AI and LLM⁴¹ have been drawing a lot more attention due to freely available chat bots. Because such models can handle large volumes of data, they are a possible tool for criminals who can obtain information about how certain offences can be committed. A likely target of criminal actors are automated systems. For example, AI could be used to more easily manipulate annual reports and tax returns to conceal shortcomings in reporting. Advanced criminal schemes using AI as a tool will probably spread to wider circles, and the development of AI services for criminal purposes could also be something that is offered for sale. It will therefore become increasingly important for public authorities to follow technological developments to understand what vulnerabilities can be exploited in future and how public authorities themselves can use the advantages of AI, for example to find systematic deviations. Moreover, public authorities need to ensure that automated selections and advanced data analysis are permitted in order to identify objects that are worth checking in terms of systematic crime.

Technological developments are also creating physical challenges. New methods of transport and new technology for the manufacture of goods can be used for criminal purposes. This enables rapid moves across ever larger distances. Examples worth mentioning include remote-controlled drones, driverless underwater vessels, 3D technology and the production of weapons.

⁴⁰ Swedish Security Service Yearbook 2022–2023.

⁴¹ LLM stands for large language models and is a program that produces text based on very large volumes of text. See also <https://it-ord.idg.se/ord/stor-sprakmodell/>.

