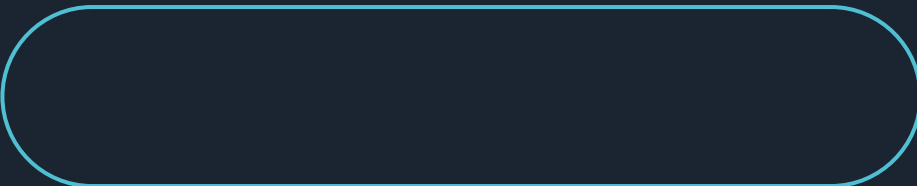
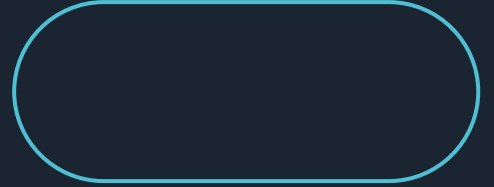




POLITIET



THE POLICE

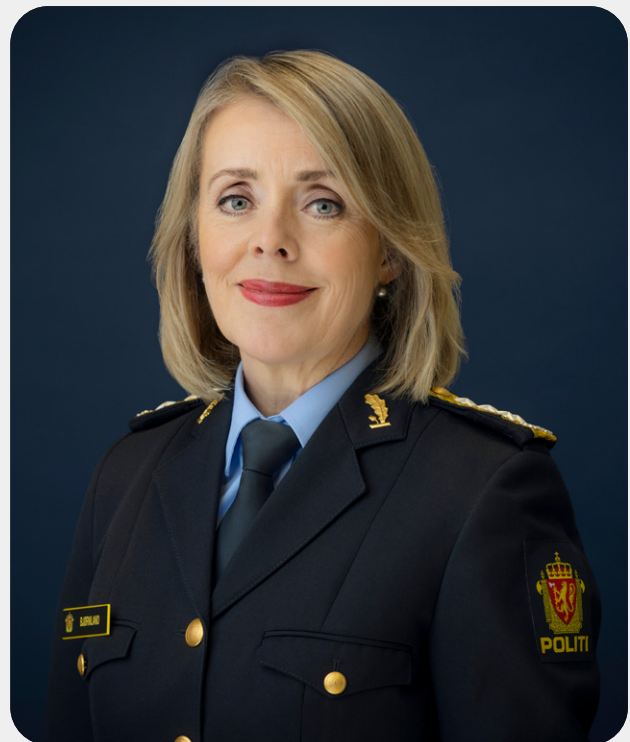
THREAT ASSESSMENT

2024

PREFACE

Ensuring the safety of society and its citizens is at the core of our mission. In an age where the line between public safety and state security is becoming erased, the police have a responsibility to communicate to political authorities and stakeholders existing threats and potential threats against our common values. The Police Threat Assessment is an important part of this communication.

A number of developments in our society is making it increasingly more difficult for the police to discharge our mission, and we are dependent upon working well with other actors to prevent crime and keep society safe and secure. There is also reason to expect that the problems and threats we will face in the future will be more complex and comprehensive than they are today. We must expect crises to coincide to a greater extent, to reinforce each other and make themselves felt across several sectors of society. Difficult times require us to prioritise. The Police Threat Assessment will help provide knowledge and serve as an important basis for priorities and our efforts to combat serious crime in the coming year.



Marie Benedicte Bjørnland
National Police Commissioner

CONTENT

01

INTRODUCTION **6**

1.1 Background and justification 8

1.2 Crime threat selection criteria 9

02

CHANGES IN THE CRIME SITUATION **10**

2.1 Overall trends in recorded crime 12

2.2 Overall trends in key crime areas which impact society's common values 13

2.3 Key drivers in crime trends 15

03

SELECTED CRIME THREATS **18**

3.1 Crime as a service helps organised crime become more professional 20

3.2 Crime exploiting legitimate structures 24

3.3 Crime in a world run by technology 26

3.4 Crime knows no boundaries 30

3.5 Crime in uncertain times 37

REFERENCES

40

01

INTRODUCTION

1.1 Background and justification

1.2 Crime threat selection criteria



1.1

BACKGROUND AND JUSTIFICATION

The Police Threat Assessment 2024 presents a selection of serious threats crime poses to our common values, threats which will make themselves strongly felt in the coming year. The purpose of the threat assessment is to help foster a shared understanding of the threat situation our society faces and form a basis for preventive action together with other actors in the private and public sectors.

The threat assessment has been prepared upon assignment from the National Police Directorate. It is based on intelligence received from the police districts and specialist agencies, as well as reports from national and international actors in the police and externally. Analysts from the NCIS, Økokrim, the National Police Immigration Service and the Norwegian ID centre have contributed in the preparation of the threat assessment.

The Police Threat Assessment 2024 is the latest in a series of annual threat assessments prepared by the National Criminal Investigation Service (NCIS) on behalf of the Norwegian police. However, this edition is different from previous years, as it mainly focuses on threats to society as a whole. One of the reasons for this is that the police are concerned that organised criminal networks established in other European countries may gain a foothold here and threaten key institutions in society. Another reason is the changes to the international security situation in Europe. In an age where the line between public safety and state security is becoming erased, the police have a responsibility to communicate

to political authorities and stakeholders existing threats and potential threats against our common values.

Unlike previous editions, this year's Police Threat Assessment does not use probability levels when making predictions, opting instead to explain them in plain text. This is to communicate our description of the crime situation in Norway in a simpler manner that may be more easily understood.

The structure of the report

The threat assessment is divided into three main sections. The first describes purpose, background and scope for the assessment. The second provides an outline of developments in a few key crime areas and describes key drivers which may have an impact on the crime situation in the coming year. The third describes a selection of crime threats which threaten our common values in various ways. The crime threats are not presented in order of priority.

1.2

CRIME THREAT SELECTION CRITERIA

The criterion for selection of the crime threats in section 3 is that they pose a threat to society as a whole. The 2024 threat assessment emphasises crime which threatens public safety, economic assets, basic structures in society and critical infrastructure and functions.

Threats to public safety are crime threats which impact where individuals choose to move in public, their activities the digital sphere or their participation in the public discourse.

Threats to economic assets mean crime threats that cause direct harm and financial loss, including the harm to society as a result of evaded taxes and distortion of competition to the detriment of legal businesses.

Threats to basic structures in society mean crime threats which undermine or exploit basic structures in society, such as a the labour market and business sector, the legal system and democratic principles.

Threats to critical infrastructure and functions mean crime threats which harm or prevent the functioning of critical infrastructure and functions. These threats may impact the state's ability to provide basic services such as health and care, electricity, water and financial services.

This focus on crime threats which impact our common values means that threats which predominantly impact individuals are not included in this year's threat assessment. The exception is where the crime has a very wide impact and therefore is considered a major threat to

society overall. Such crime includes children being subjected to sexual crime via digital platforms or fraud on a scale so large as to pose a threat to general safety and security.

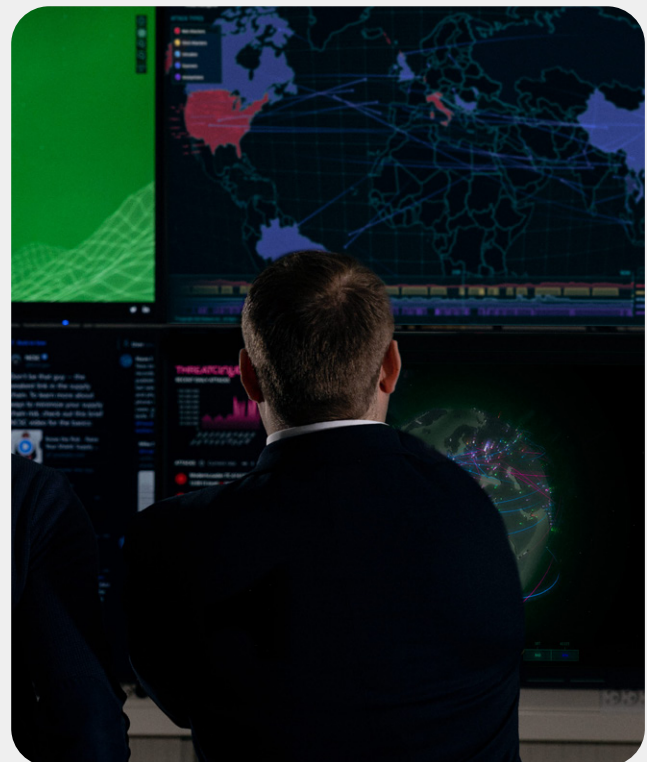


Photo: The police

02

CHANGES IN THE CRIME SITUATION

2.1 Overall development in recorded crime

2.2 Overall trends in key crime areas which impact society's common values

2.3 Key drivers in crime trends

Changes in the crime situation in Norway are described both in analyses of recorded crime and police descriptions and assessments of different crime threats impacting society.

In this section of the Police Threat Assessment, we will initially look at developments in recorded crime in Norway, based on criminal cases statistics from the police as of 31.12.23. We will then proceed to overall assessments of the threat organised crime, cybercrime and financial crime pose to society.

Society is in constant flux, and such assessments will therefore always be somewhat uncertain. In closing, we will therefore look at drivers which may impact crime in the coming year. In the latter part, we have taken our cue from the analysis framework PESTEL, which is used to identify and understand political, financial, social, technological, environmental and legal factors which impact the crime situation.



2.1

OVERALL TRENDS IN RECORDED CRIME

The number of recorded criminal cases may give an indication of the crime situation in Norway. However, these records are impacted by how willing and motivated people are to report various types of crime, categorisation practices and police efforts and priorities. In addition, changes in recorded crime in recent years may be a consequence of measures implemented during the pandemic. This is in particular the case for profit-motivated crime and violent crime.

The downward trend in the number of recorded cases which started in 2016 appears to have reversed over the past two years. However, the number of cases was lower in 2023 than in 2016. The largest categories among recorded crimes are profit-motivated crime and traffic-related offences. As regards the various crime categories, the number of recorded cases in the categories violent crime, financial crime, vandalism and profit-motivated crime for the period 2016–2023 peaked in 2023. As regards profit-motivated crime and violent crime, the decline from the pandemic has now been more than reversed.

Norway has few homicides compared with most other countries, and the number of homicides has been relatively stable over the past ten years. However, the number of homicides in 2023, at 38, was the highest since 2013.¹ 17 of the victims were killed by a current or former spouse, partner or someone they had been romantically involved with. This is 45 per cent of all victims in 2023, the second highest percentage during the ten-year period. None of the homicides in 2023 appear to be a result of conflicts in or between criminal networks.

As regards sexual crime, this category includes both physical assaults and abuse committed via the internet, as well as possession of child sexual abuse material. Sexual abuse of minors makes up a large percentage of the cases. Such abuse often takes place via digital channels and one case may involve a large number of offences and victims.

The number of recorded sexual crimes may vary a lot from year to year. Sexual crimes are a form of crime where victims are often less willing and motivated to go to the police, and when they do, they often report offences that took place a long time ago, meaning that police efforts may be decisive to uncover cases. These factors mean that the number of recorded sexual crimes provides only a partial description of the current situation.

In drug crime, the number of recorded cases have dropped in recent years and is now at half of the number of cases in 2016. However, the police are concerned about figures provided by the Norwegian Institute of Public Health, which show that twice as many young people between the ages of 16 and 30 state to have used cocaine over the past year, compared with figures from 10 years ago.² More cocaine was seized in 2023 than in the preceding 22 years combined.³

2023 also saw the highest number of crimes committed by persons under the age of 18 since 2009. More than a third of these crimes were committed by children under the age of 15. The increase is highest in the categories theft, assault, threats and vandalism. The police are noting that violence and other serious crimes have become more common among minors. The police are in particular concerned over the negative development as regards robberies, illegal carrying of knives and firearms and aggravated assault.

2.2

OVERALL TRENDS IN KEY CRIME AREAS WHICH IMPACT SOCIETY'S COMMON VALUES

The police regularly produce classified and unclassified intelligence reports on a number of crime areas. Over the past two years, a number of reports have been made public on the topics of organised crime, cybercrime and financial crime.⁴ This work has provided the police with a broad understanding of the current situation and crime trends.

Organised crime

Europe has never faced a stronger organised crime threat.⁵ Norway also faces a significant threat from organised criminals. Several criminal networks strongly motivated by profit operate in Norway, and many of them are involved in the sale, distribution and smuggling of drugs.⁶ This has been highlighted to the general public by the record seizures of cocaine made in Norway in 2023.

Organised crime may result in criminal actors both cooperating and engaging in conflicts with each other. The police see how several of the criminal networks are increasingly working with other criminals. Such cooperation is particularly conspicuous when criminals buy and sell services, assignments and specialist expertise. Specialist expertise may include anything from transport and money laundering to violent enforcement and money collection. The police have also noted that this development may result in more competition for drug markets, which has occasionally resulted in violence, also in public places.⁷

The police assess the threat from criminal networks to be significant and growing, partly due to the networks becoming more professional, growth in cross-border cooperation and increasingly complex business models. We are in particular concerned that a higher conflict level, with the threat from Swedish actors being substantial, will follow on the heels of this.

Cybercrime

Cybercrime is geographically distributed and has a wide impact. This form of crime targets both individuals, in the form of e.g. fraud and sexual crimes, and enterprises, in the form of computer intrusion, data theft and ransomware attacks. Stolen information is considered to become increasingly valuable. Small and medium-sized businesses are particularly vulnerable.

The police have seen a number of changes in cybercrime in 2023, in particular relating to geopolitical and technological factors. Cybercriminals are continuing to adapt techniques, methods, tools and strategies, partly in response to countermeasures from public authorities and private companies. However, several similarities with recent years have been observed, with the majority of cybercrimes in 2023 being opportunistic and profit-motivated.⁸ One individual crime may have more than one motivation and generate more than one type of value, e.g. both profit for cybercriminals and intelligence for state actors.



The dam at Braskereidfoss following Storm Hans. Photo: Shutterstock

The police believe the threat from cybercriminals is on the increase. The actors are acquiring more expertise and the capacity to carry out more complex operations with a greater potential for harm. Sexual crimes supported by computer systems is a persistent threat. The technological development widens the opportunities available to cybercriminals.

Financial crime

The digitalisation of society and the integration of economies and labour markets create more opportunities for cross-border financial crime. The police note how criminal networks control companies directly or indirectly, using professional actors and straw men to conceal crimes and actual ownership. At the same time, parts of the financing of the welfare state are threatened by work-related crime. There are persistent problems of undeclared wages and sales across several business sectors.

Both the police and banks are seeing the number of frauds skyrocket. The police expect fraud to increase even more, and that people of all ages and social strata will be impacted in the coming year. Fraud generates large proceeds for criminal actors, proceeds which are reinvested in new crimes. Several persons charged in Norwegian fraud cases have links to criminal networks also involved in drug-related and violent crime.⁹ Use of money mules in money-laundering operations is a growing problem and such mules have become a disposable commodity for criminals. The police expect

fraud to become a more important source of revenue for criminals and that more people will be recruited and exploited as money mules.

Environmental crime

Environmental crime is multifaceted and covers pollution, nature-related, fisheries and aquaculture crime, as well as other activities causing serious harm to ecosystems. Such crime is often motivated by financial gain or cost savings and may involve individuals, businesses and local authorities.

In Norway, the impact of climate change has made itself clearly felt in the form of more precipitation, more flooding, more avalanches and land and rockslides and shrinking glaciers.¹⁰ In autumn 2023, Storm Hans caused major local problems with environmental damage and destruction of infrastructure.

In economically tighter times, the police believe that more people may feel tempted to commit environmental crime to cut costs. The police consider that illegal destruction of nature and unpermitted land use changes may hamper our ability to handle climate change and have far more serious and costly consequences than we are seeing now.¹¹

2.3

KEY DRIVERS IN CRIME TRENDS

Society is changing constantly, and the overall assessments of crime trends set out in chapter 2.2 are therefore uncertain. In the following, we will therefore describe the drivers which may impact the crime situation in the coming year.

Crime trends in society are driven by both internal and external forces. While internal drivers are mainly motivations that are not profit-driven, such as revenge, jealousy and sexual interest in children, external drivers are factors in society which impact the crime situation and its development. Below, we have identified various external drivers which may impact the crime situation in Norway in the coming year.

International conflicts impacting the crime situation in Norway

The conflicts in Ukraine and the Middle East are examples of how war and conflict elsewhere also have consequences for Norway's interests, both domestically and abroad.

As a result of Russia's attack on Ukraine, the threats facing Norway have changed and Norway's security is being challenged in new ways. This means that so-called hybrid threats are included in the threat situation. Hybrid threats may be the result of both legal and illegal activities. Examples of such illegal activities may be sabotage, vandalism and cyberattacks. The police therefore play a key role in detecting and reporting hybrid threats.^{12,13}

The war in Ukraine has resulted in large numbers of refugees. Like refugees from other countries, Ukrainian refugees are at risk of being exploited by criminals who seek to profit from their plight through human trafficking and people smuggling. The large number of Ukrainians arriving in Norway may create opportunities for exploitation of labour and exploitation for prostitution. There are criminal networks in Norway which target refugees and try to recruit them into exploitative conditions. For example, the networks offer to organise the flight from Ukraine in return for the refugees working as prostitutes in Norway and other European countries.

The violent conflict in the Middle East is a powerful example of international conflicts generating political involvement and which may have a potential for fomenting social unrest and online hate speech.

The economic downturn may make youths more vulnerable to becoming involved in crime

2023 was a difficult year economically, with major price and interest hikes and high electricity prices. This economic climate reinforces health, social and economic disparities, causing more households to experience problems.¹⁴

In 2020–2022, more than 10 per cent of all children in Norway lived in families with persistently low incomes.¹⁵ Children growing up in low-income families may experience exclusion and are at increased risk of poorer

living conditions and lower quality of life than other children.¹⁶ This may make them vulnerable to becoming involved in profit-motivated crime and being recruited to criminal gangs. Several studies have shown that growing up in a low-income family raises the risk of becoming involved in crime as a youth.¹⁷

The connection between growing up in a low-income family and the risk of becoming involved in crime later is, however, complex, and research points to several factors which influence the life and development opportunities of children. For instance, several studies claim that the connection between low incomes and crime is more due to a low income having an impact on family relations and causing stress and unrest in the family – which may in turn influence the risk of children becoming involved in crime.¹⁸

International research also points to children and youths growing up in low-income families being more at risk of becoming victims of violence, sexual abuse and neglect. This also applies in a Norwegian and Nordic context.¹⁹

It is uncertain how the economic situation will develop in 2024, and how this development will impact the crime situation in Norway. Figures from Statistics Norway show, however, that the number of children living in households with persistently low incomes has declined over the past two years.²⁰

Technological developments create opportunities for criminals

Recent years have seen rapid technological development, also in the use of digital tools. A large share of public and private services have become digital, making society vulnerable to manipulation and extortion. Technology and technological development are therefore fundamental drivers of cybercrime.²¹ This requires legislators, the police and the private and public sectors to implement new countermeasures.

Developments in the field of artificial intelligence (AI) and anonymisation technology help create more opportunities

for criminals. AI is in constant development and a driver in raising the number of criminals operating in the digital sphere. The actors are raising their expertise and becoming increasingly efficient.²² This applies both to crime targeting computer systems and crime supported by computer systems.

AI includes technology which can help manipulate how people perceive reality. One example of this is the development of so-called deepfakes*, the making of very realistic, but fake, videos of people doing or saying things they have not. Deepfakes may be used for blackmail, identity theft and fraud, as well as for manipulation and influencing through fake news and media.²³

Further development of easily available and commercial anonymisation technologies makes it easier for criminals to act covertly in the digital space, and also to operate across international boundaries and jurisdictions.²⁴ End-to-end-encrypted messaging platforms, for instance, lower the risk of sexual offenders being discovered during sexualised contact with children and during communication with each other.

Criminal actors use various digital financial services which help them remain anonymous. Cryptocurrency market developments will impact the opportunities criminals have to commit crime such as money laundering, sexual crimes and fraud, or to conceal other criminal activity.

Hate speech on social media poses a threat to democracy

Social media have enabled far more people to make their voices heard and participate in the public discourse. The opportunity to communicate directly and at all hours has, however, also contributed to a harsher debate and an increase in hate speech and harassment, both against high-profile persons and between people who disagree on issues. Conspiracy theories and fake news spread faster than ever, weakening people's trust in each other and society.

* Deepfake is a catch-all for images, videos and audio created using artificial intelligence.

Several studies show that Norwegian politicians are increasingly subjected to threats and hate speech.²⁵ This may cause many to stop seeking elected positions and withdraw from the public discourse. Such acts and such a development may pose a threat to freedom of speech and democracy.

Issues relating to the climate and conservation of nature also lead to more polarisation

Climate change causes major harm and poses a threat to the basis for our existence. The global effects of climate change are complex and uncertain, and some areas are hit harder than others. According to the UN, 22 million people were driven from their homes by the impact of climate change in 2021.²⁶ The refugee situation creates opportunities for smuggling people to Norway. In Norway, political decisions and priorities will form the basis for conflicts between climate activists and

conservationists on one side and representatives of business interests and political decision makers on the other. Strong involvement and commitment from various groups in society may be both legal, positive and desirable. However, this may also lead to increased polarisation, which in turn may find its expression in illegal acts, both digital and physical, e.g. more hate speech.²⁷ How climate change plays out, the consequences of climate measures and influence on activists from similar groups abroad are factors which may influence whether protest will lead to illegal acts such as sabotage, vandalism and violence.

The authorities' handling of climate change, e.g. through stricter measures, may also drive environmental crime. Stricter regulation of sources of pollution and use of natural resources is also expected. Increased costs for safe handling and storage of waste may lead some to ignore requirements or make false reports to cut costs.



School climate strike outside Norway's parliament in 2019. Photo: Zhyshchynskyi Vadym / Shutterstock

03

SELECTED CRIME THREATS

M-22
POLITI

3.1 Crime as a service helps make organised crime more professional

3.2 Crime exploiting legitimate structures

3.3 Crime in a world run by technology

3.4 Crime knows no boundaries

3.5 Crime in uncertain times



This section of the report presents a selection of threats we consider put the four assets of public safety and security, financial assets, basic structures in society and critical infrastructure and functions in society at risk.

Overall, the description of the threats shows that crime is becoming more professional, that it is defined by actors who exploit the opportunities created by technological development and that criminals often operate seamlessly across geographical borders. In addition, we see how some of the crime threats arise as a result of these being times of political, financial and environmental uncertainty.



3.1

CRIME AS A SERVICE HELPS ORGANISED CRIME BECOME MORE PROFESSIONAL

In a world trending towards more complexity and functions becoming increasingly specialised, the need for knowledge and expertise in criminal networks also change. Criminal networks short of sufficient knowledge and expertise to perform specific acts are increasingly seeking such expertise from providers they can find on the dark web and elsewhere. Crime as a service is a term increasingly used to describe a development where providers of specific criminal services are becoming increasingly adept at commodifying such services. This development helps make organised crime more professional and provides criminal networks with more opportunities.

Crime as a service is a broad concept consisting of roles and services offered to all types of criminal activity – from production and recruitment to logistics and distribution.²⁸ The term is in particular associated with cybercrime, money collection, violent enforcement, logistics and money laundering. Laundering and transferring money require expertise and activities which may involve actors in both the legal and illegal economies. Various actors have specialised in money laundering and smuggling of proceeds out of the country on assignment from criminal networks in Norway. Smuggling of cash and unlicensed payment transfers are attractive services for those seeking to launder and safeguard assets.

Criminal services are bought and sold all over Norway. The police are receiving an increasing number of reports of this in connection with known criminal networks and central areas. For instance, there have been cases of

Swedish criminals engaging in violent enforcement in Norway, contracted by other criminals. Some Swedish criminal networks have strong violence and intimidation capital and the networks have become established as recognisable brand names. The development of crime as a service not only helps make organised crime more professional, it also aggravates it.

Crime as a service in cybercrime is an area in constant development

Cybercrime often requires special expertise, giving rise to a market where tools and services are sold, bought and rented out for criminal purposes. The police have observed how this market is large and growing. Innovations reach the criminal market quickly. Criminals learn from their mistakes and are at forefront of tool adoption and use.

The most prominent example of crime as a service is ransomware. This has developed into one of the most serious security risks facing the public and private sectors.²⁹ Ransomware is malware traditionally used to encrypt the victim's data. A ransom is then demanded to unlock the computer systems. The attacks are mostly conducted by criminals who have rented or bought the malware from criminal developers. The goal is to make the attacked victim pay a ransom. In addition, threats are often made to sell data and sensitive information unless the ransom is paid. The proceeds are then laundered by other criminals through several exchange services, making it to prosecute the criminals.³⁰

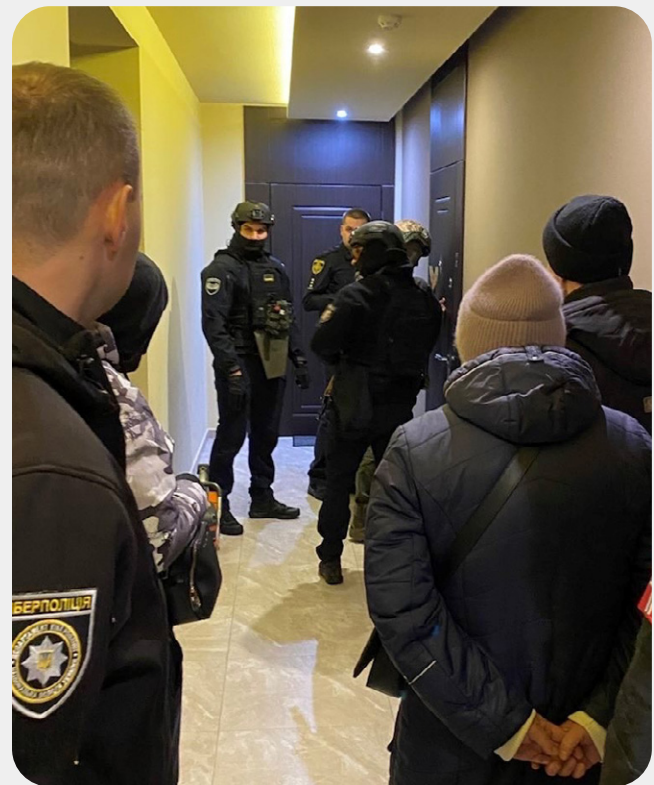
How common ransomware attacks are is uncertain. However, the number of reported ransomware attacks on Norwegian companies has declined somewhat over the past two years. Most such attacks are opportunistic and profit-motivated, but there were attacks in 2022 and 2023 which suggested a greater degree of reconnaissance and targeting. Companies which do not have the resources or have not given priority to protect their assets sufficiently, will be particularly vulnerable to attacks. These are often small or medium-sized companies. The consequences for the individual company of being subjected to a ransomware attack may therefore be significant. To some, it may mean interruption of operations and, at worst, bankruptcy.³¹

In 2023, the police observed developments in the extortion MOs of criminals attacking Norwegian companies. As an extra element to the extortion, the perpetrators stole data and then conducted a denial of service attack (see also chapter 3.5). There have also been cases of perpetrators then making contact with the company via email or telephone to extort more funds. This is called triple extortion.³²

In addition, criminals have published stolen data online. This may raise the risk of repeated attacks, as the stolen data are easily available to everyone online and can be quickly downloaded, unlike downloads from the dark web.

Login details are another commodity. They are for sale on dark web marketplaces and are used for computer intrusion and other crimes. Such login details may be

* Information stealer software is malware designed to compromise and steal information from a device. The malware can steal e.g. usernames and passwords from browsers, cookies and browser history.



The photo shows an arrest in Kyiv, where Norwegian police assisted Ukrainian police. The arrest was in connection with the ransomware attack on Norsk Hydro in 2019. Photo: The police

stolen by using so-called information stealer malware*, a type of malware that is traded on the dark web.

A third example of such commodities are zero-day vulnerabilities**, which are traded on the dark web in an environment frequented by hackers, criminals and intelligence services.³³ Zero-day vulnerabilities are only

**A zero-day vulnerability is a weak point in a piece of software which is discovered by attackers before the developer becomes aware of it.

effective for a limited time and are therefore highly valuable to criminals. Exploiting zero-day vulnerabilities requires strong expertise and efforts, which is another reason why they are so sought after.

Over the past year, the police have seen criminal actors gaining access to software developed by state actors and using it for criminal purposes. This means that advanced technology becomes widely available in criminal circles, which in turn may pose a threat to critical infrastructure. For instance, criminals may benefit from software designed to impact operational technology. OT systems are hardware and software systems used to monitor, control and manage critical infrastructure and physical processes in many industries. By attacking an OT system, criminal actors may do damage both physically and digitally, as cybercrime has both digital and analogue impact.

Recruitment of persons to carry out attacks mainly takes place in forums and venues on the dark web. Technical and linguistic expertise are sought after in cybercrime, as is expertise in human behavioural patterns, all considered critical to succeed in influencing the victim. However, criminal individuals may also carry out cyberattacks without having any prior knowledge of the software.



Photo: Shutterstock

Information about relevant tools can be obtained from like-minded people or by searching for it online. The tools are often free, and recipes on how to proceed are easily available, which in turn has a major impact on recruitment to cybercrime.

Accountants assisting criminals pose a threat to our economic system

Criminals use accountants to make companies used for financial crime appear legal. The police have information that some accountants facilitate money laundering, fictitious invoicing, tax evasion and work-related crime. They do this by creating complex corporate structures, which may help camouflage the real owners and make it harder to audit the company's finances.

There are accounting businesses who appear to offer their services exclusively to criminals (crime as a service). Examples of such services may include assisting business people to manipulate accounts, hide funds and file for bankruptcy.

Criminals who repeatedly exploit companies and then file for bankruptcy distort competition and harm the economy. Provision of credit for businesses is a cornerstone of our economic system, but entails a risk to lenders and investors. Should lenders not be able to trust that correct and complete information is provided about the true financial position of a company, fewer may be willing to invest capital or provide credit. Bankruptcy-related crime is therefore a significant threat to our economic system.



ATTACKS ON OT AND IT SYSTEMS

In November 2023, Australia's largest port operator, DP World, was subjected to a large-scale cyberattack. The attack forced DP World to take down its systems, and Australia had to close important large ports through which 40 per cent of all goods to and from Australia passes.

DP World's computer systems were taken offline and the port operator had severely limited capacity to shift containers and cargo. This example is also relevant in a Norwegian context, showing how a cyberattack might impact OT and IT systems in Norway.

Melbourne, Australia. Photo: Aerometrex Ltd / Getty



3.2

CRIME EXPLOITING LEGITIMATE STRUCTURES

By exploiting legitimate business and public-sector structures, organised criminals can more easily invest proceeds of crime and thereby increase their financial gain. By integrating the criminal activities in the legal economy, the criminal endeavours may also gain recognition and legitimacy.

The real-estate business and the fisheries industry are examples of industries where organised criminals use legitimate structures to commit financial crime. See also chapter 3.4 for how legitimate structures are exploited in goods transport.



Photo: Jacek Dylag / Unsplash

The real-estate business will remain attractive for money-laundering purposes

Cash-intensive industries are often ripe with opportunities to combine legal and illegal proceeds.³⁴ The real-estate business is an example in point. Value increases and high return on investment over many years have made the industry attractive for Norwegian and foreign capital investment. This enables criminals to invest large amounts in real estate, which is thereby integrated into the legal economy.³⁵ The amounts may be proceeds of various types of crime, including drug-related crime and work-related crime.

The approach often involves buying homes with criminal proceeds. Use of shell companies and straw men help conceal the origin of the funds. The homes are then refurbished by illegal labour paid in cash. The materials used are also paid for in cash generated by criminal acts. In this manner, the proceeds are laundered by paying the workers undeclared wages. The home appreciates in value, which in turn yields a profit to the criminals. The crime threat may also cause socio-economic loss through lost tax income and distortion of competition to the detriment of legitimate enterprises.

Fisheries crime undermines the sustainable management of fish stocks.

Norwegian seafood is considered one of Norway's most important trade goods. In 2022, the Norwegian fisheries and aquaculture industry exported 2.9 million tonnes of seafood worth a total of NOK 151.4 billion.³⁶ However, the

industry suffers from extensive fisheries crime, a term which includes environmental crime, financial crime and work-related crime. Fisheries crime is profit-motivated, distorts competition and poses a threat to the welfare state through e.g. evasion of taxes. Ultimately, the illegal activities may pose a threat to food safety and life and health. Fisheries crime takes place throughout the value chain, from sea to table.

Overfishing, quota violations and misreporting undermine sustainable management of fish stocks and harm the marine ecosystem.³⁷ Quota violations and misreporting and underreporting of catches also reduce tax revenues. Misreporting mainly takes place when the fisher delivers fish to the processing plant, either through cooperation, or the plant defrauding the fisher by misstating the weight or value of the catch.³⁸ Some market leaders have incorporated fisheries crime in their business model in several parts of the value chain.

Both professional and hobby fisher sell undeclared fish to private customers and restaurants. The sales often take place directly between buyer and seller or via digital platforms. Smuggling of catches from fishing tourism and undeclared trading in king crab may contribute to distort competition.³⁹ Illegal sale of seafood is also a threat to food safety, as it becomes impossible to ensure that hygienic standards are upheld during handling, transport and storage.



Photo: Piola666 / Getty

The fisheries industry also has problems with work-related crime and exploitation of vulnerable workers. This is the case throughout the value chain. Examples include wage theft, below-standard quarters, excess working hours, use of illegal labour and violation of driving time and rest period rules.

3.3

CRIME IN A WORLD RUN BY TECHNOLOGY

Norway has become one of the world's most digitalised countries. Like many private services, public services such as tax administration, health services and social benefits have been digitalised. In recent years, we have seen how the development of digital platforms makes it possible to create new business models linking customers and suppliers, such as in passenger transport, moving services and cleaning. Such business models may make life easier for consumers. However, it also opens the door to work-related crime, in that the employer's responsibilities are eroded and taxes etc. are not paid.⁴⁰

This technology-driven world creates new opportunities for criminals. People are put to the test when they have to navigate digital requests that may be professional fraud attempts. Criminals use many different approaches and show great creativity in their fraud attempts. Development of and the use of AI raise the threat level further in 2024.

Young people's everyday lives are also to a great extent governed by technology. This chapter shows how developments in AI and anonymisation technology create opportunities for criminals. This chapter also shows how the digital sharing culture developed in recent years has negative aspects, including the sharing of digital material showing serious violence and sexual abuse. Such sharing may have very serious repercussions for the victims.

Artificial intelligence may lead to more children and young people being subjected to profit-motivated sexual extortion

Children and young people's exploration of their own sexuality to a large extent takes place online, making them particularly vulnerable to various forms of sexual abuse. The police have noted an increase in reports of profit-motivated sexual extortion. There is reason to believe that a significant number of such cases go unreported.⁴¹ Overall, this type of extortion poses a threat to the safety of children and young people in the digital space.

Sexual extortion with a financial motive is often carried out by professional criminals located abroad. Well-organised call centres operating globally have been uncovered. The extortion takes place using false accounts, with victims being deceived into taking nude photos of themselves or recording themselves performing sexual acts. The victim is then extorted for money in return for the perpetrators not sharing the material with e.g. friends, family members or social media followers of the victim. There are examples of boys and young men having paid several thousand NOK as a result of such extortion. The sums demanded vary, mainly from NOK 5000 to 20,000, and payment often takes place in cryptocurrency. Those who pay are generally met by new demands, and in some cases the material has been shared in spite of payment being made. The police have also seen several cases where the threats have been carried out when the victim does not pay up.

The police have observed how the extortion is becoming more aggressive, with new and even more cynical methods being used. The demands are for larger amounts and victims have become younger in recent years. There are reports of victims as young as 13 and 14. Most of the victims are boys and young men between the ages of 15 and 25, but girls are also targeted. The extortion takes place on most social media frequented by young people. Snapchat, Instagram and Discord are among the most frequently used platforms.

The continuous development of AI creates greater opportunities for the threat actors. Firstly, it enables criminals to use regular photos of victims to make fake nude photos. It will therefore no longer be necessary to win the victim's confidence to gain access to nude photos for use in extortion.⁴² The police have information that AI is being used to generate sexual material with the intent of engaging in financially motivated extortion.

Secondly, AI may be used to make the selection of potential extortion victims more effective and targeted. Through use of translation tools, anyone can communicate in any language and adapt their wording to the age of the victims. Internationally, there are reports of AI being used to establish contact and extort minors.⁴³

Thirdly, AI may lead non-professional actors without an affiliation with organised crime to engage in such crimes. A recent example from Spain involved young boys manipulating photos of young girls aged 11-17 using AI software and then distributing fake nudes of the girls through WhatsApp and Telegram.⁴⁴

Use of AI will lead to more children and young people being subjected to financially motivated sexual extortion. Such exploitation can cause significant harm to the victim and is associated with severe self-recrimination and shame.⁴⁵ Several victims have killed themselves after being subjected to such extortion, also in Norway.⁴⁶

More sharing of severe sexual material and videos showing violence

In recent years, a culture of sharing has developed where minors are increasingly sharing disturbing content on social media. The content includes both severe sexual material and videos showing violence. The sharing is rapid and extensive, and the consequences can be very serious for the victims.⁴⁷ Uncertainty as regards where the material has been shared and who has seen it can cause mental strain and impact life in school and otherwise.

As regards sharing of sexual material, the police have noted that videos showing rape and intercourse are frequently shared on social media. The police receive many tip-offs about young people downloading and/or sharing sexual abuse material, including sexual material of their peers. Children as young as 11 and 12 share or have photos of themselves shared. Both boys and girls share sexualised material, but boys are more often involved in the sharing. The sharers are connected to each other, either through school or in other ways. In several cases, the sharers of sexualised material have also recorded the material and are shown in it.

Recent years have seen the creation of an increasing number of so-called 'exposed' accounts, closed accounts where images and videos are shared, often content submitted by the the account followers. These accounts are most common on Snapchat, but exist also on other social media such as TikTok and Instagram. There are also minors among those who create and/or follow such accounts.

'Exposed' accounts are mainly used to spread rumours, harass people and the like, but also for sharing pornography and sexual abuse material.⁴⁸ Over time, the material shared has become more severe. Examples of shared content includes private photos of minors in various degrees of nudity, children in sexualised situations and people performing sexual acts on animals. Exposed accounts are also used to share videos showing rape and severe sexual abuse of children.

Sharing of videos showing violence also takes place via such exposed accounts. Young people all over the Norway record violent acts and share the resulting videos on social media. This may both normalise violence and generate new violent acts.⁴⁹ In several parts of the country, the police have noted an increased propensity for violence with perpetrators becoming younger. In some youth communities, the threshold for using violence is low, and some violent acts are stated to be the result of spreading of rumours, provocative behaviour and disagreements.

The police expect the sharing culture to result in use of violence becoming more normal and that more serious violent acts will be committed against and by young people. Serious violent incidents not only have consequences for the victims, it may also make society in general less safe.

Sharing and increased exposure to more severe sexual material may change attitudes and normalise sexual abuse among young people. The development can thereby be a driver for new sexual crimes.^{50,51}

Criminals with international connections defraud Norwegian nationals

Both the police and banks are seeing the number of frauds skyrocket. The problem has now reached a scale where it is on the verge of becoming a public safety issue. Private individuals, organisations and companies all suffer major financial losses. The police, banks and IT security departments are forced to spend significant resources to uncover fraud.⁵²

The perpetrators employ various approaches and exhibit varying degrees of organisation. The frauds are often very professional in their execution, with the perpetrators having become experts in various functions.

The approach of calling from a spoofed telephone number and posing as the victim's bank or the police is particularly common. Text messages are also used to

gain access to the victim's online bank and card details. The text message will often be included in the message log from the genuine actor on the victim's mobile phone, which in turn will more easily deceive the victim. Such exploitation of telecom infrastructure vulnerabilities may weaken people's confidence in private and public enterprises and their digital security solutions.

In recent years, several perpetrators in fraud cases have had ties to other serious crime and criminal networks, including drug-related and violent crime. Some key actors are also involved in robberies and illegal possession of firearms. There are also obvious similarities between fraud cases in Norway and Sweden. Fraud through car loans and credit without security involve transnational criminal groupings which are also involved in drug crime and people smuggling.⁵³



INVESTMENT FRAUD AND ROMANCE SCAMS

Many Norwegians are subjected to investment fraud and romance scams. Investment fraud is considered the most serious form of fraud targeting private individuals and often involves people being tricked into investing in more or less worthless shares and cryptocurrency. Romance scams trick people into transferring money or making their account available to someone they have established a relationship with, often through dating apps.

Over the first six months of 2023, the police recorded losses exceeding NOK 150 million from investment fraud and romance scams. The perpetrators in both investment frauds and romance scams are often abroad.

*Spoofing means that the person receiving the call sees the number the perpetrators want them to see.



USE OF DEEPPFAKE IN FRAUD

Many associate deepfake technology primarily with visual deception, but the technology can also be used to fake audio. One problem that is likely to become more prevalent going forward, is the combination of automation and tailored attacks.

A hypothetical example of automation combined with a tailored attack would be a call centre with computers making automated calls. The computer calls a private individual to record the person's voice under the pretence of conducting a survey. Data leaks from social media are then used to find the person's friends. The computer then calls these friends using spoofing technology, and it appears that the call is coming from the person who was recorded.

In addition, AI is used to make the voice sound like the recorded person. In reality, the caller is a computer trying to collect personal data. This approach enables criminals to reach more potential victims quicker. There have also been cases where perpetrators have used ChatGPT, and criminals are showing a growing interest in this. This is likely to lead to a significant increase in the number of attempted frauds.

In early January 2024, the internet was rife with compromising deepfakes of the artist Taylor Swift.

Photo: Brian Friedman / Shutterstock



3.4

CRIME KNOWS NO BOUNDARIES

Norway's borders are more than 2500 km long, and 20 km of it is the Schengen external border with Russia. The Norwegian maritime border is also the Schengen external border. This chapter is about how Norway is faced with transnational criminal networks which operate relatively seamlessly across national borders and between continents. Such networks pose a threat to Europe, a threat Europol claims has never been higher.⁵⁴

The criminal networks engage in various forms of crime. Serious drug-related crime is prominent, but they are also involved in violent crime, human trafficking, work-related crime, fraud, money laundering and smuggling of both legal and illegal goods. In several parts of Norway, the police also know of criminal actors involved in importation and distribution of illegal firearms. In many of the cases, the networks are run by organisers and leaders who reside abroad – also in countries with no extradition treaties with Norway or in countries which do not extradite their own citizens.

Organised crime is mainly covert. However, organised crime is considered one of the major crime threats to public safety.⁵⁵ This is due to their business models becoming increasingly complex, more professional and with frequent replacement of collaboration partners. Very simplified, the criminal landscape may be considered a criminal ecosystem or a loosely connected network of professional criminals, where cross-border cooperation is both shifting and systematic. Organised crime also threatens public safety through violent acts in the public sphere, as seen in Sweden, the Netherlands and Belgium.

Criminal networks will increasingly use Norway as a transit country for narcotic drugs

Criminal networks involved in drug smuggling have traditionally used goods transport by road to smuggle drugs into Norway. In 2023, however, the police observed an increase in drugs seized from cargo vessels. Three record cocaine seizures totalling 2 tonnes* were all smuggled into Norway in ship containers originating from South America. In all three cases, the criminal networks used legitimate food transport logistics and attempted to conceal the drugs among regular goods. In addition, more than 100 kg of cocaine attached to the hull of a ship in port in Western Norway was seized in April 2023. These drugs also originated in South America.⁵⁶

Norway has a long coastline that is hard to monitor. Enormous distances, long and branching fjords and many potential ports of call make maritime monitoring very resource-intensive and difficult. Norwegian ports therefore appear attractive entry points for criminal networks seeking to smuggle cocaine in containers and cargo vessels from South America.⁵⁷

Being an attractive point of entry carries a potential threat, both to public safety and to key structures in society. Antwerp and Rotterdam, Europe's most popular transit ports for trans-Atlantic cocaine smuggling,⁵⁸ have seen an increase in violent crime (including use of firearms and explosives) in connection with drug market rivalry between criminal networks.⁵⁹

*712 kg, 803 kg and 503 kg, respectively.

This violence has also caused collateral injuries and deaths – with criminal networks engaged in cocaine smuggling having killed innocent third parties in the Netherlands to prevent testimonies in a trial.⁶⁰ Other threats include corruption among port workers, vessel crew members, customs officials, police officers and the staff of other authorities.⁶¹ These are relevant threats and vulnerabilities also in a Norwegian and Nordic context.⁶²




DRUG SEIZURES IN 2023

In 2023, the number of cases in which drugs were seized increased by 7 per cent compared with the preceding year. Previously, this figure had declined every year since 2014. The amount of cocaine seized is several tens of times larger than normal, and the cocaine seized is of a very high purity. Several seizures of very potent opioids, such as nitazenes and fentanyl, were also made in 2023. Such synthetic drugs are often very potent, increasing the risk of overdoses.⁶³ In parallel with new synthetic opioids reaching the Norwegian drug market, international heroin production has plummeted. The Taliban banned all opium production in Afghanistan in 2022. With Afghanistan being the source of almost all heroin consumed in Europe, this may result in

users of heroin and other opioids seeking synthetic alternatives.⁶⁴

Narcotic drugs have generally retailed at high prices in the illegal market. The police estimate retail prices to range from NOK 300,000 to 500,000 for 1 kg of cocaine, NOK 100,000 to 250,000 for 1 kg of heroin and NOK 50,000 to 100,000 for 1 kg of marijuana. In comparison, 1 kg of cocaine costs around NOK 30,000 in the South American countries⁶⁵ where the production takes place, around 10 per cent of the Norwegian retail price. This illustrates how lucrative drugs can be for criminal organisations.

RETAIL PRICES IN NORWAY

	1 KG OF COCAINE		1 KG OF HEROIN		1 KG OF MARIJUANA
	300 000 – 500 000		100 000 – 250 000		50 000 – 100 000

TRANSNATIONAL CRIMINAL NETWORKS IN NORWAY

The threat posed by transnational criminal networks operating in or targeting Norway will make itself felt in different ways in 2024. Moroccan criminal networks will pose a significant threat as regards smuggling and distribution of cannabis and cocaine to and in Norway. Albanian-speaking criminal networks are expected to pose a significant threat as regards smuggling and distribution of cocaine. Lithuanian criminal networks provide important transport and logistics services to other criminal networks in Europe and the Nordic countries and will continue to smuggle large quantities of drugs to Norway.

The Norwegian police know that some drug crime networks targeting Norway have transatlantic connections providing them with direct access to the production of cocaine in South America. Among the large networks in Europe, Albanian and Moroccan actors stand out with their direct connections to South America. These

networks straddle large parts of the value chain, from the actors controlling the production to the distribution and retail side of the business in European cities.

This lucrative business is dominated by some of Europe's largest criminal networks, including networks from Italy, Morocco and the Balkans.

Criminal networks and actors will generally work with others where there is a profit to be made, regardless of national, ethnic, cultural and religious affiliations. Criminal networks operate in a criminal value chain similar to those in legitimate business models. From the head organiser level in drug networks in Colombia, Italy, Albania and Morocco to street dealers in Norway, profits dictate operations, actions and the ever-changing constellations of who is working with whom. Although the threat posed by the transnational criminal networks is primarily covert, the goods traded are worth so much that it impacts safety and security in society as a whole.



COLOMBIA



NORWAY

LITHUANIA

ITALY

ALBANIA

MOROCCO

Increased activity by Swedish criminal networks in Norway may result in more violent incidents

In recent years, Sweden has seen an increase in serious and fatal violent incidents resulting from drug-related rivalry between criminal networks. Some of the networks have strong violence and intimidation capital, and have established themselves as recognisable brands.

In 2023, all Norwegian police districts recorded activity relating to Swedish criminal actors. The activity is mainly related to drugs and gaining access to Norwegian drug markets. How much activity there is varies by district. Some Swedish criminal networks have been active in the Norwegian drug market for years and have well-established relationships with Norwegian networks. In other cases, the Swedish criminal networks or actors are in the process of establishing themselves in the drug market in the police district. In some districts, the only links to known Swedish criminal networks are stand-alone drug seizures.

There have been cases of Swedish criminals engaging in violent enforcement in Norway, both as contract assignments and to support their own business. More activity in Norway may result in conflict with existing criminal networks in Norway or existing conflicts in Sweden playing out here.

The activity of Swedish criminal actors in Norway will increase in the coming year, primarily in drug-related crime. Norway appears as an attractive market to these actors due to established connections and higher potential profits from higher street prices.⁶⁶ Considering developments in recent years and the resulting media attention relating to gang crime in Sweden, the presence of Swedish criminal actors in Norway may impact how safe the public feels.

In the struggle for market shares and control over turf in Sweden, the criminal networks have deliberately used inexperienced children under the age of criminal responsibility to commit murders and serious violence. Recruitment takes place on social media and encrypted



Handover of drugs. Photo: The police

communications platforms. No such cynical and targeted recruitment of children to perform violent acts in Norway has been observed. However, the apparent normalisation of violence and substance abuse, combined with the how available this normalisation is through social media, make young people vulnerable to such recruitment.

Criminal networks exploit legitimate structures to smuggle people into Norway

Over the past two years, there has been an increase in the number of persons smuggled into Norway, also with the aid of criminal networks. Several Norwegian networks have become more professional over time, in that they e.g. use legitimate structures such as companies to carry out the people smuggling. Some of the networks have engaged in people smuggling over several years and have proven to be highly adaptive when faced with measures implemented by the police or other authorities.

People smuggling is lucrative, with prices per person

smuggled into Norway range from NOK 50,000 to 250,000. The networks smuggling people into Norway for them to seek asylum, use several methods. The most common methods are for ID documents to be misused to smuggle migrants by air from southern Europe or to smuggle them by road.

The networks which facilitate legalising the smuggled person's stay so they can work, do this by using false documents showing education or work experience. Applying for a Norwegian residence permit for work requires extensive ID and education documentation, in addition to a specific job offer from an employer in Norway. The networks operate in several business sectors, and both foreign and domestic actors are involved in the various processes. Such crime poses a threat to life and health, in that persons without the necessary skills work in e.g. car repair shops and on construction sites. Those smuggled may also be exploited for labour after arrival in Norway.

Some of the people-smuggling networks can also be linked to other serious crime, such as drug-related, financial and work-related crime. They mostly operate in the greater Oslo region, but also in other parts of Norway.

Smuggling of cash, animals and goods in and out of Norway may threaten public health and finance crime

Information held by the police indicate that smuggling of cash and goods in and out of Norway can be linked to international criminal networks.⁶⁷ Smuggling of illegal or undeclared goods lead to loss of tax revenues and may pose a danger to public safety and health.

NOK 8 to 10 billion in cash is declared upon entry to Norway every year, but the amount declared upon leaving Norway is significantly lower. A large share of the difference of cash going in and out is smuggled out of the country. Several actors are involved in cross-border circulation of Norwegian banknotes. Cash is smuggled out of Norway by money mules on international flights, in lorries carrying legal goods and in private cars.⁶⁸

The actors who smuggle cash out of Norway are often part of a larger international network of money changers who cooperate to make transfers when needed. The purpose may be to use cash as payment for illegal goods, to launder money or finance terrorism.

Illegal import of foodstuffs pose a significant threat to food safety in Norway. This is due to the risk that the foodstuffs have been handled and stored incorrectly, and that it is hard to trace their actual origin. This is particularly serious when involving the sale of meat, cheese and seafood. The hygiene requirements relating to labelling, handling and storage are strict to protect consumers against illness.

Smuggling of pets and threatened species into Norway poses a threat to public health.^{69,70} Animals smuggled into Norway may carry diseases and parasites that are potentially lethal to humans and animals, such as rabies and tapeworms.⁷¹ The networks which smuggle pets and threatened species also appear to often be involved in other forms of crime.

Several cases have been uncovered where Norwegian actors known to be involved in other forms of crime import and resell counterfeit goods in Norway, i.e. intellectual property (IPR) crime. Such goods are typically designer clothing, cosmetics and household goods. In the EU, IPR crime used by criminal networks to finance other serious crime is a well-known problem.⁷² Whether IPR crime is used to finance other organised crime in Norway is unknown.



MISUSE OF NORWEGIAN IDENTITIES

Every year more than 30,000 Norwegian passports are reported lost or stolen. Some of the passports are deliberately stolen from tourists in major European cities. This, combined with a large industry producing false documents, provides criminals with easy access to identities they can use to commit various forms of crime.

An increasing number of Norwegians become victims of digital identity fraud. Large volumes of personal data belonging to Norwegian nationals are for sale on the dark web and on end-to-end-encrypted messaging platforms.

Criminals can use such data to conceal criminal activities, e.g. by creating cryptocurrency accounts to hide money trails or taking out subscriptions to communicate covertly.

According to Europol, the money from this criminal industry is used to finance and strengthen complex criminal networks, including networks involved in financial fraud, drug trafficking, human trafficking and terrorism.

The historic Bryggen area in Bergen. Photo: The police



3.5

CRIME IN UNCERTAIN TIMES

When entering 2024, we are facing a world that is more uncertain and unpredictable in political, financial and environmental terms than has been the case for a long time. This chapter covers crime that may be viewed, fully or partly, as the result of these uncertain times. Such crime may threaten society's common values, such as freedom of speech, general safety in the public sphere and conservation of nature to protect us against the impact of climate change. One of the threats highlighted in this chapter also shows how activism may play out in a digital world, including how politically motivated groups can engage in digital vandalism through denial-of-service attacks.

Threats and hate speech may lead to polarisation and limit participation in the public discourse

Freedom of speech has a strong position in Norway compared with most other countries.⁷³ Freedom of speech is a basic principle of Norwegian law, and although the Penal Code bans some forms of aggravated hate speech, most utterances are permitted.

Threats and hate speech have a broad impact and negatively affect both society and individuals, regardless of being punishable or not. The potential effects include exclusion, polarisation and limiting participation in the public discourse. In this manner, threats and hate speech may undermine democracy.

Slightly more than 400 cases of hate speech were reported to the police in 2023. Most of the cases involve statements targeting a person's skin colour or ethnicity. Over the past two years, and in particular after the terrorist attack on 25 June 2022, the police have, however, noted an increase in received reports of hate speech against queer people. Whether this is due to an actual increase in such hate speech or a greater willingness to report, is uncertain. This increase persisted into 2023.

Hate speech is also aimed at trans people, a topic on which the public discourse appears to be highly polarised. There has been an explosive increase in the number of tweets about trans people over the past few years, from around 1500 in 2018 to almost 24,000 in 2022. Almost half the tweets were critical of trans people. Both trans persons and Pride were increasingly mentioned in critical terms on both Twitter and Facebook during this period.⁷⁴

Many politicians are also subjected to hate speech and/or threats. This mostly happens on social media. A recent survey of the how common hate speech and threats against local politicians is show that more than 40 per cent of those who had experienced this had changed their behaviours, some by moderating their political message. Well over half of those represented in this group have considered giving up politics.⁷⁵

* Denial-of-service attacks are most often carried out by overloading the network capacity or other resources or by blocking a service or function.

Stronger cooperation between politically motivated groupings may raise the threat against Norway

Denial-of-service attacks are easy to carry out and easily available and are most commonly used by politically motivated criminal groups operating online – so-called hackers. ** Such attacks are considered digital vandalism but cause limited damage as the attacks are generally intended to influence political processes and do not target websites directly linked to operations or internal systems of an enterprise.⁷⁶

Over the past year, a development has been observed where hacker groups are increasingly seeking to work with each other. Such cooperation may raise the overall expertise and capacity of the groups and make them better able to commit complex and damaging cybercrimes – e.g. computer intrusion, data theft and digital vandalism. The Norwegian National Security Authority (NSM) reports a concern that this form of attack is being developed to use of more sophisticated techniques and that it may be used to target vulnerabilities in enterprises' networks. NSM also refers to the fact that experiences from abroad show that attacks have become more sophisticated and harder to detect and protect against.⁷⁷

More cooperation between hacker groups may pose a growing threat to Norway, as such groupings are often behind denial-of-service attacks. The police have noted a massive increase in such digital vandalism over the past year, carried out by various political groups. The attacks have primarily been aimed at the technology, business sectors and public administration sectors, but the recent year has seen an increase in pro-Russian actors attacking enterprises in the transport, finance and health sectors. The latter sectors have not previously been targeted to any great extent.⁷⁸ It is assumed that western support for Ukraine has led to more cooperation and strengthened solidarity between these groups.

One possible cause of the increase in denial-of-service attacks against Norwegian targets may be Norway's clear support for Ukraine. As Norway is playing a key role, both

** Such as KillNet, Anonymous Sudan and REvil.

by sending military equipment for use on the front lines and through political processes in connection with NATO, Norway becomes a target for politically motivated criminals.

Tensions in diaspora communities can result in violent confrontations

Over the past year, several rallies, protest marches etc. have resulted in violence between opposed parties. These incidents predominantly arise from conflicts between or internally in diaspora communities in Norway. Some of those involved have also spontaneously directed their aggression against the police during these rallies etc.

These partly violent rallies have often taken place in connection with the legal gatherings and protest marches of other groupings. By trying to curb the freedom of speech of groups they oppose, the participants in such counter-rallies threaten democratic principles such as the freedom of speech and the freedom of assembly. Similar developments have also been noted in other European countries, often with even more use of violence. Also in those cases, violent aggression has been directed at the police.

There are reports of serious threats in diaspora communities, without such threats necessarily being reported to the police. Language barriers and lack of confidence in the authorities may be among the reasons they are not reported.

The conflicts in these communities have the potential to trigger more violent incidents in later confrontations.

Potentially high profits and low detection risk lead to illegal destruction of nature and land use changes

Illegal destruction of nature and land use changes take place all over Norway. Violations take place on private property and in protected areas, mountains, wetlands, forests and the littoral. They include illegal building, road construction, digging and blasting, removal and depositing of mass, terrain changes and logging. Violations vary

widely, both as regards type and seriousness. In many cases, natural areas and ecosystems are subjected to permanent or long-term damage. In addition, a broad range of vulnerable nature types and animal and plant species are affected. Few cases are reported to the police.

The violations are committed by private individuals, businesses and local authorities. Many of them take place in connection with or in the vicinity of existing buildings or in connection with other construction work. Cases involving illegal depositing of mass and illegal changes to the use of buildings may pose a risk to people's life and health. In 2022, several local authorities were reported for violations of the Planning and Building Act. As the competent planning authority, local authorities decide most construction permit applications. The risk of violations probably rises when the local authority is represented on both sides of the table, as planning authority and developer. It may weaken the general deterrent effect of the provisions when the competent authority finds itself reported to the police for crimes, which may in turn undermine structures in society and democratic principles. Illegal destruction of nature and land use changes also take place in connection with other forms of crime, including corruption cases in local authorities.⁷⁹

Most of those reported to the police are private individuals who commit violations on their own property. Illegal destruction and construction may yield financial gains as the property becomes worth more and time and costs for application processing are saved. In several cases, the perpetrators are repeat offenders and demonstrate deliberate intent, which may be due to the costs saved and profits gained being significant and detection risk low. Securing a dispensation is by some considered a formality, and some probably count on it being "easier to ask for forgiveness than permission". Discovery of violations often have very limited consequences.⁸⁰

Climate change may reinforce the consequences of illegal logging

Climate change in the form of more precipitation and more extreme weather may cause significant infrastructure

damage and at worst put lives at risk.⁸¹ Forests help delay run-off from water catchment areas and thereby provide protection against the effects of climate change by preventing flooding, erosion and rock and mudslides. In spite of the regimes that are in place to protect vulnerable and valuable natural areas, illegal logging of valuable forests still takes place. Should the current rate of illegal logging continue, we may become less able to handle climate change in the future. This will result in illegal logging having far more serious and costly consequences than those we already see.⁸²

Both the Forestry Act and the Nature Diversity Act aim to protect nature and remedy the damage resulting from violations. The violations include logging not preceded by statutory environmental mapping and logging of key biotopes in spite of them having been mapped and recorded.

The number of reported crimes is low, and most cases involving illegal logging appear to be minor when seen in isolation. Overall, however, such violations may cause serious damage. This is due to the damage in most cases being irreversible.⁸³ In most cases, the violations have few or minimal consequences for the perpetrator. Much indicates that neither the rules themselves nor their enforcement have a deterring effect. Low detection risk and the profit potential are factors which may result in illegal logging remaining a problem in Norway.



February 2024, the Trøndelag County Governor's Office reported illegal logging in Bymarka nature reserve in Trondheim to the police. Photo: Carina Ulsund/ Statsforvalteren i Trøndelag

*An area which is particularly important to biological diversity.

REFERENCES

1. Kripos. 2024. *Nasjonal drapsoversikt – drap i Norge 2013-2023*.
2. Folkehelseinstituttet. 2023. *Narkotikabruk i Norge* (09.02.2023).
3. Kripos. 2023b. *Narkotika- og dopingstatistikk 2023*.
4. Kripos. 2023a. *Cyberkriminalitet 2023*; Kripos. 2023c. *Nasjonal trusselvurdering. Nasjonal operasjon rettet mot kriminelle nettverk (KN)*. Offentlig versjon; Kripos. 2023d. *Generativ kunstig intelligens og cyberkriminalitet*; Økokrim. 2022a. *Økokrims trusselvurdering 2022*.
5. Europol. 2023a. *The other side of the coin. An analysis of Financial and Economic Crime*; Euronews. 2021. *Europe has reached a 'breaking point' over organised crime, says Europol* (12.04.21).
6. Kripos. 2023c.
7. Kripos. 2023c.
8. Kripos. 2023a.
9. Økokrim. 2023f. *Bedrageri – et samfunnsproblem*.
10. Klima- og miljødepartementet. 2021. *Slik kan vi tilpasse oss klimaendringene* (22.10.2021).
11. Økokrim. 2023c. *Ulovleg hogst*.
12. NOU 2023:17. *Nå er det alvor - Rustet for en usikker fremtid*.
13. NOU 2023:14. *Forsvarskommisjonen av 2021. Forsvar for fred og frihet*.
14. Helsedirektoratet. 2023. *Kunnskapsoppsummering om ulikheter i helse og livskvalitet i Norge siden 2014 – sammendrag*.
15. Statistisk sentralbyrå. 2024. *Færre barn lever i familier med lavinntekt* (18.1.24).
16. Statistisk sentralbyrå. 2023. *Hvor mange er fattige i Norge?* (14.6.23).
17. Savage. 2009. *The Development of Persistent Criminality*. Oxford University Press.
18. NOVA. 2018. *Muligheter og hindringer for barn i lavinntektsfamilier. En kunnskapsoppsummering*. Rapport 11-2018.
19. NOVA. 2018.
20. Statistisk Sentralbyrå. 2024.
21. Kripos. 2023a.
22. Kripos. 2023d.
23. Kripos. 2023d.
24. Kripos. 2023a.
25. Ipsos. 2020. *Hatefulle ytringer og trusler mot lokale folkevalgte. Rettslige rammer, rettspraksis og kommunesektorens praksis*; Ipsos. 2023. *Hatytringer, trusler og desinformasjon mot folkevalgte*.
26. FN. 2023. *Providing legal options to protect the human rights of persons displaced across international borders due to climate change*. A/HRC/53/34.
27. Forsvarets forskningsinstitutt. 2021. *Samfunnsutvikling frem mot 2030*. Rapport 21/01132.
28. Europol. 2021. *Serious and Organised Crime Threat Assessment (SOCTA)*.
29. Norsk senter for informasjonssikring (NorSIS). 2023. *Hva er løsepengeangrep?* (02.08.2022).
30. Kripos. 2023a.
31. NSM. 2023. *Nasjonalt digitalt risikobilde 2023*.
32. Recorded Future. 2023. *Threat Analysis 2022 Annual Report*.
33. NSM. 2023.
34. Europol. 2023a.

35. Finanstilsynet. 2023. *Risikovurdering 2023. Hvitvasking og terrorfinansiering.*
36. Norges Sjømatråd. 2023. *Norge eksporterte sjømat for 151,4 milliarder kroner i 2022* (06.11.2023).
37. NOU 2019:21. *Framtidens fiskerikontroll. Nærings- og fiskeridepartementet.*
38. Politiet. 2023a. *Politiets trusselvurdering 2023.*
39. Økokrim. 2022a.
40. Økokrim. 2023a. *Status arbeidsmarkedskriminalitet juni 2023.*
41. TV2. 2023. *POLITIET ADVARER: Gutter blir lurt og presset for penger: – Alvorlig* (23.7.23).
42. ECPAT. 2023. *Då tog "hon" en screen og allt började. En rapport om sexuell utpressning av barn i økonomisk syfte med særskilt fokus på pojkars utsatthet.*
43. Thorn, Stroebel og Portnoff. 2023. *Generative ML and CSAM: Implications and Mitigations.* Stanford: Internet Observatory. Cyber Policy Center.
44. NRK. 2023c. *Kunstig intelligens brukt til å generere falske nakenbilder av mindreårige jenter i Spania* (25.09.2023).
45. ECPAT. 2023.
46. Kripos. 2019. *Seksuell utnyttelse av barn og unge over internett.*
47. Kripos. 2022. *Ungdom henges ut på nett: Deling av ulovlig og bekymringsverdig materiale av barn og ungdom.*
48. Kripos. 2022.
49. Politiet. 2023b. *DELE=DELTA: Om deling av voldsvideoer*
50. Kripos. 2019.
51. Oslo Politidistrikt. 2018. *Trender i kriminalitet 2018-2021. Digitale og globale utfordringer.*
52. Økokrim. 2022b. *Økokrims årsrapport 2022.*
53. NRK. 2023a. *I grenseland* (22.01.2023).
54. Europol. 2021.
55. Europakommisjonen. 2021. *EU-strategi for bekjempelse av organisert kriminalitet 2021-2025.*
56. NRK. 2023b. *Slik avslørte politiet og Tolletaten rekordbeslaget* (19.11.2023).
57. Kripos. 2023c.
58. Politico. 2023a. *Europe's got a problem' – Drug violence grips Belgium's second largest city;*
- Euronews. 2023. *Antwerp takes over from Rotterdam as Europe's leading port for cocaine seizures* (10.01.2023).
59. Europol. 2023b. *Criminal networks in EU ports: Risks and challenges for law enforcement.* Joint report of Europol and the Security Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven and Rotterdam; EMCDDA. 2022. *'Cocaine: increasingly attractive for a wide range of criminal networks'.*
60. EMCDDA. 2022.
61. Global Initiative Against Transnational Organized Crime & InSight Crime. 2021. *The Cocaine Pipeline to Europe;* Europol. 2023b.
62. Kripos. 2023c.
63. Kripos. 2023b.
64. UNODC. 2023. *Afghanistan opium cultivation in 2023 declined 95 per cent following drug ban: new UNODC survey.* Press release.
65. GI-TOC & InSightCrime. 2021.
66. Kripos. 2023c.
67. Økokrim. 2022a.
68. Økokrim. 2023b. *Nå er det NOK – kontanter i den kriminelle økonomien.*
69. Økokrim. 2022a.
70. Mattilsynet. 2022. *Mattilsynet deltar i europeisk storaksjon mot smugling av kjæledyr* (03.11.2022).
71. Mattilsynet. 2023. *Hvordan unngå å kjøpe ulovlig innført hund* (21.03.2023).
72. Europol. 2022. *Intellectual Property Crime Threat Assessment 2022.*
73. NOU 2022:9. *En åpen og opplyst offentlig samtale – Ytringsfrihetskommisjonens utredning.*
74. Analyse & Tall. 2023. *Ytringsklimaet for skeive på Twitter og Facebook.*
75. Ipsos. 2023.
76. Kripos. 2023a.
77. NSM. 2023.
78. NSM. 2023.
79. Økokrim. 2023d. *Ulovlige naturinngrep og arealendringer.*
80. Økokrim. 2023d.
81. Økokrim. 2023e. *Miljøkrim, nr.1.* 2023.
82. Økokrim. 2023c.
83. Økokrim. 2023c.



POLITIET

The Police Threat Assessment 2024

Published by: Kripos

politiet.no/trusselvurdering