POLITIET

POLICE

THREAT ASSESSMENT 2025

NORWAY

PREFACE

The main responsibilities of the police are to maintain law and order, investigate and prevent crimes. We will be the citizens' protector and ensure public safety and security. For us to succeed, the citizens need to have faith in the police and feel safe in their everyday lives. The police's mission is twofold: We must fight the high volumes of everyday crime, while also stopping the more professional and organised actors who commit crime that threatens our society.

The criminal landscape is in a state of flux. Criminals operate seamlessly across national borders, leveraging technology and structures in a society defined by a high degree of trust and digitisation. This creates vulnerabilities which are exploited by criminal networks and actors and places high demands on the ability of the police to adapt, develop new techniques and apply new technology.

But we cannot solve these challenges on our own. Close cooperation with other authorities, the private sector and civil society is essential to fight crime and prevent new threats. Such cooperation requires a shared understanding of the crime threats we will be faced with in the year to come. We need to be flexible, forward-looking and goal-oriented in our efforts. The Police Threat Assessment is intended to give better insight into developments in crime and the challenges we are faced with. Through this knowledge sharing, we strengthen our overall ability to prevent, detect and fight threats to society.

National Police Commissioner

Håkon Skulstad

CONTENTS

01 INTRODUCTION

Photo: The police

1.1

BACKGROUND AND PURPOSE

The Police Threat Assessment is an annual report reflecting the police's most up-to-date and comprehensive understanding of the Norwegian crime picture. This year's report focuses on crime threats to society in particular. This is crime which in various ways threatens public safety, security, our shared assets and values and is deemed a particular challenge in the year to come. The purpose of the Threat Assessment is to promote a shared public understanding of the threat picture faced by society.

There are several reasons why this year's report focuses on the crime which threatens society. The world is evolving at a fast pace. War and conflict, high costs of living and digitisation not only affect the ways we live our lives, but also the way crime is committed. Not least, crime is evolving at an ever faster pace in this globalised and digital era. Modern-day crime is more complex and complicated than in the past, and the police rely on cooperation with a broad spectrum of players to accomplish our mission. This Threat Assessment is hence also intended as a tool for strengthening the police's preventative partnerships with private- and public-sector players.

The Police Threat Assessment has three parts: Part 1 describes the purpose, background and scope. The chapter also discusses some key drivers which have influenced crime over the past year, and which the police believe will continue to do so in the year to come. Part 2 describes the overall evolution of the crime picture in Norway over the past year, based on recorded crime. Part 3 presents a selection of crime threats which in various ways endanger the things we value in our society. Not ranked by severity, they collectively constitute crime which threatens society, and which the police wish to highlight.

The Threat Assessment is prepared by Norway's National Criminal Investigation Service (NCIS) on behalf of the National Police Directorate and the wider Norwegian Police Service. Its content is based on intelligence received from all local police districts and specialist police agencies as well as reports from national and international police and non-police players.

Police Threat Assessment - Norway 2025 Menu

1.2

HOW THE POLICE DEFINE CRIME WHICH THREATENS SOCIETY

The police work systematically to determine what crime threaten society. The criterion for the selection of the specific crime threats in Part 3 is that they constitute a threat to society as a whole. This year's Threat Assessment focuses on crime which threatens *public safety, economic assets, fundamental societal structures, critical infrastructure and public functions, and nature, animal welfare and cultural heritage.*

Threats to public safety are defined as crime threats that affect the movement of individuals in public space, their activity in digital space or their participation in public debate.

Threats to economic assets are defined as crime threats that cause direct harm and economic loss, including macro-economic losses through tax evasion, distortion of competition and outcompeting of businesses.

Threats to fundamental societal structures are defined as crime threats undermining or exploiting fundamental societal structures such as a fair labour market and business environment, legal systems and democratic principles.

Threats to critical infrastructure and public functions are defined as crime threats damaging or obstructing critical infrastructure and public functions. Such crime may compromise the state's ability to continue to deliver basic public services such as health services, electricity, water and financial services.

Threats to nature, the environment and animal welfare are defined as crime threatening biodiversity, the climate and ecosystems. Consequences include the loss of animal lives and poor animal welfare. Also included are threats to cultural heritage, such as illegal trade in cultural objects, vandalism and other offences that threaten our shared cultural heritage.

Photo: Unsplash

1.3

KEY DRIVERS OF CRIME

It is essential for the police to understand the societal drivers behind the emergence and spread of crime. In our ever-changing world, societal developments both *influence* and *are influenced* by crime. There are internal and external drivers. Internal drivers are primarily motivational factors such as financial gain, revenge or jealousy, whereas external drivers are social factors. If we understand the drivers, we can be more effective in preventing and combating crime, and over time create a safer society.

PESTEL AS A FRAMEWORK

In this work, we have used the analytical framework PESTEL, which can be used to identify and understand how political, economic, social, technological, environmental and legal factors can influence the crime picture.

PESTEL is a widely used socio-analytical method which helps users understand which components affect complex dynamics, and how it happens. [1]

An analysis of the key drivers of crime gives insight into what influences criminals' actions and how they can lower the risk of detection and succeed. This chapter describes different *external drivers* which may provide a better understanding of the past year's crime picture and crime which will threaten society in the year to come.

Security policy factors influencing the crime picture in Norway

The national crime picture may be influenced by the international security policy situation. Entering 2025, several major conflicts, e.g. in Ukraine, the Middle East and Africa, dominate the news. War, conflict and regional instability produce flows of refugees and other irregular migration. Refugees tend to be in a vulnerable position and to have fewer options in terms of seeking or getting help. Criminal networks and opportunistic actors may take advantage of their situation through e.g. people smuggling, human trafficking or identity abuse. Women and children run the added risk of being sexually abused.

Measures implemented as a result of superpower rivalry include sanctions and trade restrictions. In Norway, the police have indications that lone actors are assisting entities on the EU list of sanctioned entities, breaching the ban on selling, supplying, transferring or exporting certain currencies and commodities. In business and industry, there are actors trading in sanctioned commodities or services through obscured company structures. The police are aware of cases involving hundreds of million NOK in industries such as shipping and fisheries.[2]

Police Threat Assessment - Norway 2025 Menu

The ongoing international conflicts and political processes can engage people politically, but also create a backdrop for hate crime and social unrest, which may manifest itself in public expressions of opinion, such as protests. The majority of the many protests in Norway over the past year took place without incident. However, there were isolated cases of violence between opponents and against the police over the past year.

«The young people of today are witnessing darkness in mid-day, with acts of war and suffering we did not think was possible in Ukraine, the Middle East, in Sudan.»

Norway's Prime Minister, Jonas Gahr Støre, in his New Year Speech 2024.[3]

Russian attack on a residential building in Dnipro, Ukraine. Photo: Shutterstock

Crime or use of hybrid means?

In a world of high tensions and geopolitical insecurity, there is also increasing opportunity for state actors to use hybrid means which have the potential to threaten Norway's sovereignty, population, territory, vital societal functions and infrastructure.[4] These are acts committed by or on behalf of a state actor, often with the aim of achieving long-term strategic objectives. The Norwegian Police Security Service and the Intelligence Service both pointed out, in their unclassified threat assessments for 2025, that state actors use proxies to achieve their objectives.[5,6] They may include different types of criminal actors.

Research literature describes how hybrid threats are carried out to an extent and a level of severity which are below the threshold for warfare, seen in isolation and collectively. They are incidents which occur in peacetime, covertly or overtly, by use of both legal and illegal means.[7] Examples of such activity include drone activity in no-fly zones such as airports or military camps, or theft, damage to property and vandalism targeting different sectors or critical infrastructure, e.g. the energy and telecommunications sector.

Some of the activities are carried out in digital space. One example is the theft of sensitive information of potential benefit to state actors. The professionalisation of organised crime and the use of crime-as-a-service may lead to collaboration between criminal and state actors. It is often extremely demanding, in digital as well as physical space, to establish the underlying motives for crime.

The literature describes a grey area below the threshold of armed conflict where it may be unclear which authority is responsible for managing such threats. From a police perspective, this is misleading. There is no grey area, only a blue area, which is the police's sphere of responsibility. In that perspective, the police have a unique and vital role in the detection of incidents which may be attributed to the use of hybrid means.

> *There is no grey area – only a blue area, which is the police's sphere of responsibility.*

Police Threat Assessment - Norway 2025 Menu

The advances of technology make things easier for criminals

The advances of technology and digitisation have made society more interconnected and efficient, but also more vulnerable. This interconnectedness being global, it directly and indirectly increases the ability of criminal actors to attack Norwegian interests in and outside Norway without being physically present. The Norwegian Government's digitisation policy aims to make Norway the world's most digitised country, where tasks are solved digitally wherever possible.[8] For the authorities, it is, however, demanding to continuously enact laws that keep pace with the advances of technology.[9]

While increased digitisation offers numerous benefits, it also offers criminals opportunities to develop more sophisticated methods. It may be challenging for the public to keep up with the fast digital developments, where it is becoming harder and harder to separate fabricated from genuine information. This is especially true for the developments in artificial intelligence and anonymisation technology, which let users generate e.g. so-called deepfakes and synthetic sexual abuse images. Another consequence is the development of new, sophisticated fraud methods which results in higher numbers of fraud victims. In 2024, three out of four fraud cases were for instance committed by digital means, or partially so.

ARTIFICIAL INTELLIGENCE: IN DEVELOPMENT

Over the past year, artificial intelligence has become progressively more available to the public through services such as OpenAI's ChatGPT or Microsoft's Copilot. Although estimates for the pace of development of artificial intelligence vary, leading technology experts seem to agree that there is an exponential development in capability and complexity. For example, Elon Must stated, during a conference in Saudi Arabia in October 2024, that artificial intelligence generally improves tenfold each year, and so will be 10,000 better within four years.[10]

Artificial intelligence is not restricted to openly available tools, software and organisations, who generally cooperate with police authorities. Criminals have a high ability to exploit, and develop their own, artificial intelligence to their own ends.[11]

Photo: The police

Social media and smartphones are important parts of young people's lives, but raise their risk of being exposed to crime or becoming victims. Exposure to and sharing of e.g. violent videos or sexual images may contribute to a normalisation of such acts.[12] Social media may also lower the threshold for committing drug crime, because openly available digital platforms act as arenas for buying and selling narcotic drugs. The same is true for recruitment to other types of crime.

Political processes as arenas for hate speech, confrontations and malign influence activity

Democracy and freedom of speech have strong positions in Norway, with the associated demonstrations and expressions of opinion in physical and digital space. Such arenas for debate are, however, at risk of being challenged, not just by the extremist statements of individuals, but also by the malign influence activities of foreign states. A debate dominated by the extremist statements of a minority tends to make others shy away from participating in the public debate.

The trend observed in the Western world, a polarised political landscape, is to some extent reflected in digital arenas in Norway.[13,14,15,16] 2025 will see general and Sami parliamentary elections. In that connection, the advances of technology in e.g. artificial intelligence will be useful to actors intending to confuse or manipulate voters.[17]

In addition, political elections and priorities that concern interest groups are often accompanied by various forms of demonstrations and activism. This may entail vandalism, sabotage or violent confrontations.

Challenges in the Norwegian economy give rise to crime

Norway is an affluent country with low rates of unemployment and a generally high level of welfare. But due to high inflation and high interest rates, many people's financial situation has deteriorated, both in households and companies. Figures from 2023 show that nearly 22% of households in Norway cannot tolerate an unforeseen expense.[18] Higher interest rates have resulted in higher monthly mortgage repayments, and the rising prices of groceries and other necessities have made it harder for many people to make ends meet. Furthermore, there are indications that economic and social inequalities in Norway are increasing, and that social mobility has been reduced.[19] This trend may drive more actors to tax crime or other forms of economic crime.[20]

Children and young people from low-income families are less able to take advantage of the various opportunities in education, leisure activities and employment. Social exclusion and marginalisation are among a range of factors which may put children and youths more at risk of becoming involved in profit-motivated crime and being recruited to criminal networks. Studies also show that youths raised in families with unemployment and disability pension are more likely to be physically abused than their peers.[21,22]

Climate change has a range of social impacts

The global climate is becoming progressively warmer. Extreme natural events such as wildfires, extreme rainfalls and mudslides are on the rise, destroying the livelihoods of millions. Climate change has both local and global impacts. In Norway, too, climate change threatens our nature and environment.

Warmer waters and more acidic oceans, combined with other external impacts, may change the representation of species in marine ecosystems. In both coastal and marine regions, we can expect a higher representation of southern species spreading north and disturbing food chains.[23] Greater insecurity about the development of fish stocks may affect quota allocations, which may in turn weaken the livelihoods of fishermen. Changed quotas may lead to more fisheries crime in the form of breach of quota rules.

Climate change also entails the expansion or shrinking of types of nature, threatening biodiversity. Some Norwegian endangered species, animals as well as plants, are highly sought-after by collectors and as such exposed to illegal international trade.

Flood in Gol, 2023. Photo: Shutterstock

02 CRIME OVER THE PAST YEAR

Citizens should feel safe and trust the police to do their job. For that we need to understand how crime has evolved overall, and take our cues from that insight. A broad analysis of crime and its drivers allows the the police to form an opinion on which crime threatens society.

Photo: The police

The police's database of criminal cases, where all reported crimes are recorded, give an indication of the evolution of the Norwegian crime picture. External factors potentially impacting the figures must be taken into account when reading them. Such factors include citizens' inclination to report crimes, reporting policies in the public and private sectors, changes to police recording practices and variations in police efforts and priorities over time.

The volumes of recorded crime will also be affected by cultural perspectives and society's attitudes towards crime. A culture of silence and internal justice in criminal groups and other communities will lead to an under-reporting reflected in statistics. To assemble a general picture of the evolution of crime in Norway, this report considers recorded crime in the context of multiple other knowledge products. They include intelligence products developed by the police regarding specific actors or which provide in-depth analyses of the development of different crime threats and phenomena.

Figures from the police's database of criminal cases over the past seven years first show a few years of decrease in the number of recorded crimes. However, this trend turned in 2022, and there has been an upward trend since then. One explanation may be that we as a society have put the pandemic behind us. Acquisitive and traffic offences top the list of reported cases, as for the past two years. Below we will present the major crime areas and their development. They include crimes involving minors, i.e. those below 18 years of age.[24]

CRIME STATISTICS

The main source of the crime statistics presented in this chapter is police operations statistics. These statistics are based on information from the police case handling system and retrieved from the Criminal Cases Database. The source data have not undergone the same error testing and quality control as Statistics Norway's official crime statistics and may therefore contain errors and deficiencies.

2.1

DRUG CRIME

For the purposes of this report, drug crime means the consumption, purchase, sale, storage or importation of drugs legally classified as narcotic or performance enhancing drugs. Recorded drug offences had gone down for several years, but this trend turned in 2022. Over the past two years, the police have seen a steady increase in recorded drug crime.[25] Those involved in drug crime do not necessarily identify as victims, and so there is no incentive to report. For this reason, recorded cases or quantities seized are just one of many indicators of the prevalence of drug use, depending heavily on the priorities of the authorities and reporting policies. Therefore, supplementary sources such as research and self-reporting surveys may provide a more complete picture of citizens' drug use.

Police drug seizures were dominated by cannabis and cocaine i 2024. As with the number of criminal cases, quantities seized will also vary greatly based on circumstances and variation in police priorities and use of resources. The purity level of cannabis has gone up considerably over the past few years; that of cocaine remains extremely high.[26]

A large proportion of recorded drug cases over the past two years concerned drugs sent by post, which partly explains the increase in recorded cases. During the same time period, Customs reported a considerable increase in cannabis seizures from courier and postal parcels. The most common sender countries are the USA and Canada, followed by Thailand. This trends reflects the fact that these countries have legalised cannabis. The size of the seizures indicate that the drugs are intended for resale in Norway.[27]

Surveillance photo, Tønsberg Airport. Photo: The police

Self-reporting surveys in 2024 show that the clear majority of drug users, in terms of proportion and actual numbers, live in urban areas, especially the major cities. Drug users may be any age, from their mid-teens to their sixties, but the clear majority are aged 16–25, with consumption gradually decreasing with age.[28] Comparisons with other European countries show that Norway is now among the countries with

Photo: The police

the highest average consumption of cocaine.[29] In the cities, the use of cannabis and to some extent cocaine has become fairly normalised in some age groups and social circles, although the great majority are only occasional users.[30] It seems that just a limited share of cocaine users commit other crime or are unable to work due to their consumption, but the trend is still concerning in a long-term perspective because cocaine is extremely addictive.[31]

The heroin market in Europe has been significantly affected and the supply reduced, over the past year, as a result of the new Afghan regime's close-down of opium production. Users perceive the quality as poorer and purity levels are more variable. Combined with reduced availability, these developments have made heroin less attractive to users. In turn, prices have plummeted.[32] The police in several countries are concerned that heroin addicts will turn to more potent synthetic opioids.[33]

This is confirmed by a rise in seizures of highly potent synthetic opoids of the category nitazenes in Norway over the past year. Even though seizures are still few compared with other drug categories, there have been several nitazene overdoses and overdose deaths.[34,35] 2023 saw a total of 323 overdose deaths across all drug types, the highest number recorded since 2001.[36] There has been an upward trend in overdose deaths since 2013.[37]

There is also a recorded increase in seizures of some types of illegal anabolic steroids in 2024, compared to 2023. The increase appears to primarily concern postal parcels. This can probably be explained by the rising acceptance of the use of performance-enhancing drugs, especially among young people.[38]

2.2

VIOLENT CRIME

Violent crime is a collective term which covers threats, physical assault, bodily harm, domestic violence and homicide etc.[39] Violent crime increased slightly from 2023 to 2024. The majority of offences were physical assaults and threats. Recorded cases of domestic violence are up, following a year-on-year decrease from 2017 to 2022.

The year 2024 started with a high number of homicides, 11 just in January.[40] The average over the past decade was 28 homicides per year. The number of homicides was above average in 2023 and 2024, with both years seeing a higher number of homicides in a domestic context. 24 of the 37 homicide victims in 2024 were killed by an intimate partner or family member (65%). In five of these cases, more than one person were killed.[41]

There is also a recorded increase in homicide attempts over the past five years. This probably reflects changed case coding policies in the police as well as an actual increase compared to previous years. The police are seeing signs of a shift in homicide attempts by young people. The violence appears more planned, more people are present during the incidents, and more of them carry weapons, most often knives.

Violent crime has risen among the under 18s over the past years. More than 80% of offenders are boys, and the majority of reports concern physical assault and threats. A higher reporting tendency or a changed understanding of what can be considered violent crime probably results in more reports .[42] There are also reports of a culture of silence among youths where many are afraid to report crimes or testify for fear of repercussions. This may complicate the investigation of violent crimes, and cases go unreported.

Photo: The police

2.3

ECONOMIC CRIME

Economic crime covers fraud, tax fraud, corruption, money laundering and work-related crime etc. Government funds, private individuals and businesses are all victims of this profit-motivated type of crime. Reports increased by 12% from 2023 to 2024, and thus economic crimes had the highest increase on 2023.

Fraud constituted 85% of economic crimes in 2024, up from 77% in 2020. Despite this rise, there is believed to be under-reporting. Around three out of four reported frauds were digital.

There were about ten corruption cases, the great majority concerned local authority employees taking bribes in connection with the sale or purchase of goods or services from businesses. Corruption takes place in the private and public sectors and has harmful effects beyond the financial damage. It may undermine citizens' trust in government institutions, employees and processes.[43] Centrally placed individuals who take bribes risk becoming involved in further offences.[44]

Work-related crime is the breach of a wide range of employment-related rules and regulations in Norway. The crime tends to be organised, it distorts competition and undermines important parts of society. Repeat offenders of work-related crime often commit tax crimes and insolvency crimes, too. Money laundering reports have risen steadily in recent years. Proceeds from a high number of crimes need to be laundered to be used and integrated into the legal economy. Despite this, there are few recorded crimes. In recent years, the use of money mules has gone up. They are individuals who let criminals use their bank accounts for money laundering purposes after being threatened or paid by them.

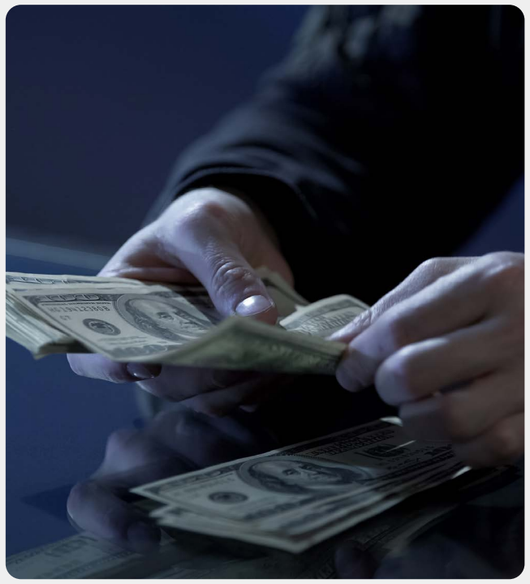


Photo: Getty Images

2.4

ACQUISITIVE CRIME

Acquisitive crime is crime in order to acquire for oneself or others benefits such as money or valuables. It includes theft, misappropriation, receiving proceeds of crime and robbery.[45]

Acquisitive crime has the highest reporting rates, making up 36% of all recorded offences in 2024. The increase was especially in pickpocketing and vehicle-taking. To process claims, insurance companies generally demand evidence that the offence has been reported to the police, which may make victims more inclined to report and ultimately affect crime statistics.

Acquisitive offences committed by under 18s have risen over the past two years, with a slight decrease in 2024 compared to 2023. Petty thefts, including shoplifting, in the age group 13–17, top the list of reported offences. Boys are behind just over 60% of the offences.

Robberies have gone up slightly over the past two years, with a large proportion being perpetrated by under 18s. It reflects the increase in so-called youth robberies, especially in the Oslo region. Statistics show that a few young repeat offenders commit the majority of the offences.[46] However, it must be noted that the data for the robbery statistics is uncertain, as it varies how robbery is coded in police systems, and because there is substantial under-reporting due to factors including an established culture of fear and silence among the relevant youth groups.

Photo: The police

2.5

ENVIRONMENTAL CRIME

Environmental crime is crime against nature, flora and fauna, art and cultural heritage, aquaculture, animal welfare and the working environment. The majority of environmental offences in 2024 concerned nature, fisheries and animal welfare. Reported environmental offences have been stable over the past few years, with 2024 seeing the lowest numbers in the last five-year period. The crime causes serious harm to individuals, the environment and ecosystems, is often motivated by financial gain or cost savings and may be committed by individuals, businesses or local authorities.

Illegal waste management is a nature conservation offence which may result in pollution and the release of hazardous substances for years to come. Internationally, this type of crime is distinguished by its exploitation of legal structures.[47] Other nature conservation offences are disturbance of wildlife through illegal hunting, trade in endangered species, illegal motorised traffic in nature and the illegal destruction of nature, such as unpermitted construction in the protected 100m zone along the Norwegian coast. The number of reports have decreased slightly in recent years. That may be due to the new power of the Norwegian Environment Agency to impose penalties, meaning that fewer such cases are recorded by the police.

A rising number of reports concern adventure tourism involving reckless use of nature and the disturbance of wildlife.[48,49] Adventure tourism also includes fishing, an activity which is strictly regulated through quotas and export rules. Customs have, in recent years, made several large seizures of fish from people attempting to smuggle it out of Norway.[50]

The majority of breaches of environmental regulations which apply to the fisheries industry are circumvention of quota rules and environmental harm caused by the fish farming industry, such as plastic waste pollution and a negative impact on wildfish stocks.

Photo: Getty Images

2.6

CYBERCRIME

Cybercrime covers a broad spectrum of offences ranging from cyber-dependent to cyber-enabled crime, comprising any offence committed by means of or facilitated by information and communication technology, including computer systems, networks, devices and software, as mentioned in chapter 1.3.[51] Typical offences in cybercrime are computer intrusion, theft of sensitive information, illegal sharing or sale of stolen data, use of ransomware to extort money from victims, as well as denial-of-service attacks to disturb or disrupt digital services.[52] Cyber-dependent crime is crime committed against computer systems, while cyber-enabled crime is traditional crime facilitated by computer-systems such as fraud, sexual offences against children or distribution of drugs.[53]

The Penal Code is technology-neutral, for the most part. That makes it hard to extract accurate information from the police's Database of Criminal Cases on the share of offences which can be classified as cybercrime. Such offences will be recorded as different crime categories in the database. But a look at the modus operandi of the recorded cases can tell us something about the development. To the extent that the police learn about cases involving e.g. ransomware and computer intrusion, they have increased over the past years. However, there is believed to be considerable under-reporting of incidents. One of the reasons why digital attacks on Norwegian businesses are not reported by victims may be fear of damaging their reputation and competitiveness if the incident becomes public knowledge.

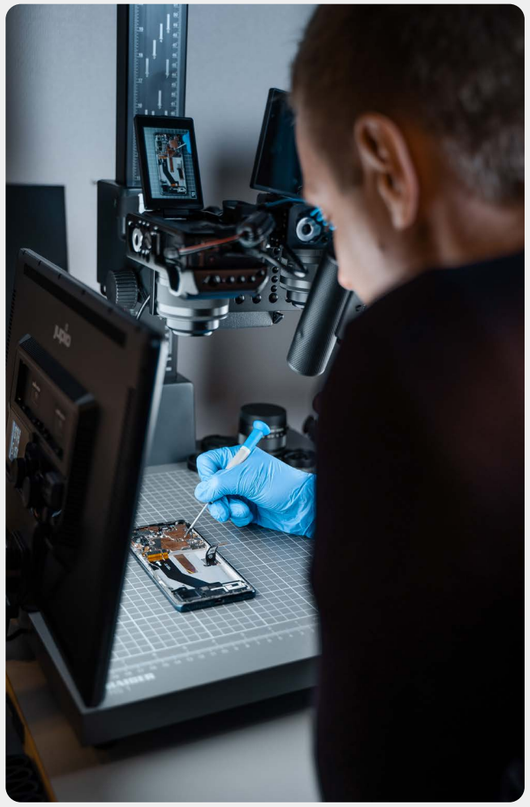


Photo: The police

2.7

SEXUAL OFFENCES

Sexual offences cover rape, sexual assault, indecent exposure, sexual touching and possession or production of child sexual abuse images or sexual images of children etc. In 2024, there was a small decrease on 2023. Children are victims in about 50% of cases.

Sexual offences are committed both online and in the real world, and one offender can have a very high number of victims. The police know that the inclination to report such cases is lower than for most other crimes. Many sexual abuse cases are, for various reasons, only reported years after they happened, and police efforts are frequently crucial in uncovering the offences.

According to the 2023 Ungvold ("young violence") study, sexual violence among children and teenagers has increased. The prevalence of almost every type of sexual violence measured by the study had doubled from 2015 to 2023, among girls and boys alike. The report also shows that digital platforms play a key part in sexual offences among children and teenagers. The most common offence was threats or pressure to make someone send sexual images or videos.[54]

Sexual offences are often internet-related, ranging from the sharing of sexual abuse material to cyber-enabled rapes. Of cases reported in 2024 where the identity of the victim was known, about 50% were minors under 14. Digital sexual abuse may be challenging to uncover because offenders may use anonymisation services in their contact with the minors. In many cases, hands-on sexual abuse is the culmination of an approach online, sometimes following a long period of grooming. However, the police know that many minors suffer hands-on sexual abuse without previous online grooming. They are abused by relatives or people in their community.

Digital developments have also enabled live-streamed distant child sexual abuse, requested and paid for by people in Norway. Such crimes are rarely reported; the sexual abuse of children from extremely deprived families is bought by predators from their own homes. The police have strong reasons to believe that several Norwegians travel abroad every year to abuse children, complicating prosecution in Norway. In some poor countries, such abuse may be considered a necessary evil – because the child is helping the family survive.[55]

Photo: The police

2.8

TRAFFICKING IN HUMAN BEINGS

Trafficking in human beings is when someone by force, threats, taking advantage of someone's vulnerable position or other improper conduct, forces, exploits or misleads someone for the purpose of e.g. prostitution, forced labour, forced services or crime. It takes place in public space, in private homes and in the workplace. The actors involved in human trafficking may be criminal networks or individuals, in some cases persons close to the victim.

Cases reported have been fairly stable over the past five years, at about 25–35 reports per year. The majority of reports are exploitation for prostitution or sexual purposes, but the proportion of forced labour and forced services has increased gradually over a five-year period. The low reporting figures are a clear indication of considerable under-reporting.

Victims of human trafficking will rarely identify as victims to authorities or organisations. Emotional, financial and social dependence on the network and family are vulnerabilities that can be taken advantage of. For those reasons, victims may not seek help, feeling that the exploitation is legitimate or fearing reprisals or social exclusion.[56] These factors make victims less likely to go to the police.

Photo: Getty Images

2.9

HATE CRIME

Hate crime is criminal offences motivated by hate or hostility towards an individual or a group based on ethnicity, religion, beliefs, sexual orientation, disability, gender identity or gender expression.[57] The incidents generally occur in random encounters between strangers. Very few of the offences are committed by members of extremist or radical groups. They tend not be pre-planned, but rather prejudices that manifest themselves when people meet.[58]

Recorded hate crime reports have risen over the past decade. Whether this reflects an actual rise in incidents, a higher inclination to report, or a better overview by the police is not known. The majority of the criminal cases concern racist hate speech. Reports of hate crime against disabled people have been stable in recent years.

There is believed to be considerable under-reporting. It is a challenge to convince victims to report incidents, as the offences against disabled people are often committed by their carers.

The volume of tip-offs received from the public online is affected by current events, as they raise people's awareness and their tendency to alert the police. Especially after the terrorist attack on the gay bar in Oslo on 25 June 2022, the police have seen an increase in reports of hate crime against the LHBT+ community. As for religion, Moslems are most at risk of hate crime. The police observed an increase in reported cases of anti-Semitism after 7 October 2023, but by the end of 2024, their number has returned to average.

Police Threat Assessment - Norway 2025 Menu

High level of security during the Pride celebrations. Photo: The police

03 CRIME THAT WILL THREATEN SOCIETY IN THE YEAR TO COME

Based on our knowledge of the drivers of crime and how crime has evolved in general over the past year, we will in this part present selected crimes which threaten society, and which will be the focus of police attention in the time to come. The crime threatens society because it endangers our shared assets and values (see chapter 1.2).

Photo: The police

3.1

ORGANISED CRIME IN A GLOBAL AND DIGITAL ERA

Every single day, Norway's societal structures are affected and threatened by criminal networks. With globalisation, transnational crime increases, and criminal networks cooperate both on opportunistic and systematic bases across national borders and continents. The advances of digital technology have amplified the opportunities of organised crime and made their activities more efficient. Anonymisation technology, particularly in communications and payment services, is used to plan, recruit, request, carry out and pay for criminal offences. The platforms may lower the risk of detection, allowing criminals to keep a safe distance from each other and their crimes.

Over the past year, the public has, through the media, gained insight into conflicts, threats and violence within and between criminal networks in Norway. Violence or threats of violence are commonly used means in organised crime, within networks, and against fellow criminals and victims. The majority of criminal networks in Europe use violence and threats for their criminal enterprises.[59] Several networks are cynical in their recruitment and exploitation of minors to carry out offences, e.g. violence-as-a-service. The organised crime and visible use of violence may make people feel less safe, in physical and digital space, and in that sense threatens our society.

> *Its size and structure tell us little about the threat posed by a network.*

NETWORKS COMMITTING ORGANISED CRIME

Criminal networks are born and survive through their ability to generate profit for its members, who are not necessarily united by nationality, ethnicity, cultural or religious ties. Their structures are complex, vary greatly, and may be short-lived or long-lived. Some networks have a stable, hierarchical structure with a strong leadership based on family ties, while others are centred around a few individuals who work as a team for pragmatic rather than ideological reasons.[60]

In many cases, networks are controlled by organisers and leaders abroad, including in countries which have no extradition treaties with Norway or do not extradite their own nationals. Its size and structure tell us little about the threat posed by a network.

Where networks lack the knowledge and expertise to carry out specific acts, they are now more likely to procure that expertise from providers on the dark web, among other places. This has triggered the development of crime-as-a-service, the provision of specialist criminal services for money. This makes organised crime more professional and amplifies the opportunities of criminal networks.

According to Europol, more than 86% of the most threatening criminal networks in Europe have created their own or infiltrated other legal business structures. By exploiting legal business structures, networks cover up their criminal activities and profits, making it a challenge to distinguish legal from illegal business. This undermines trust in public institutions, business and industry and the justice system, and drains resources from our economy as a nation.[61]

Photo: Shutterstock

Drug networks play a key role in the development of organised crime in Norway

The most prominent criminal networks in Norway engage in large-scale drug crime, with many of them also committing other crimes to cover up and facilitate their criminal activities. They include economic crime, violent crime, people smuggling, human trafficking, arms trade and cybercrime. Several of the drug networks in Norway have been established for years, and are extremely resilient and adaptable. Drug crime is often organised and accompanied by other types of crime, representing a persistent and growing threat to key societal structures.

The drug networks are often described based on nationality, activities and structure, but in actual fact, the criminal landscape is more fragmented and complex. Drug criminals collaborate across national borders wherever profit opportunities exist, meaning that networks and individuals may be competitors and enemies, but also partners as needed. Facilitators, specialists and hired hands are integral parts of the process. Local networks become local markets for global distribution chains. The police are seeing increasing levels of professionalism and collaboration between different networks and independent criminals. Independent criminals have no particular network affiliation or loyalty, but will cooperate wherever there are opportunities to make money. They operate dynamically between networks.

> *Local networks become local markets for global distribution chains.*

Police Threat Assessment - Norway 2025 Menu

The advances of digital technology in e.g. social media, encrypted communications platforms and cryptocurrency have improved networks' circumstances and enabled the development of a digital system for drug activities. The police have observed a trend whereby drug sales are moving from specialised, obscure services on the dark web to publicly available communication platforms such as Snapchat, Telegram and Signal. The trend is nation-wide.

Several of the seller accounts on social media have a professional and well-organised appearance, presenting a wide selection, price lists and advertisements with language and emojis adapted to specific customer segments. Both individuals and criminal networks operate seller accounts. The drugs are delivered by dropping them off in specific locations or by domestic post. So in the space of a few minutes, anyone can buy and sell drugs on the open web, just like any other online retailer.

The internet has become a large part of most people's everyday lives, with 94% of citizens going online at least once on an average day. The most popular social media platform among those under 35 in 2023 was for instance Snapchat.[62] The exposure to drugs on offer on social media and the distance between the seller and the buyer create a lower perceived detection risk. It may give rise to a perception that it is harmless, and lower the threshold for drug crime in society.

Communication platforms and social media also act as criminal meeting places and arenas for recruitment. Sellers recruit other sellers, and people are hired to carry out violence related to the drug activities. These digital tools have many users and so act as an extended recruitment arena for networks and their drug activities.

Drug seizure. Photo: The police

CRIMINALS WILL CONTINUE TO BE ACTIVE ACROSS THE NORDIC COUNTRIES

The police are seeing that criminal networks and actors are collaborating on organised crime across the Nordic countries, a threat expected to rise in the time to come. The system-threatening and very serious crime which used to be largely confined to Sweden has over the past year evolved, and to some extent spread to Norway and the other Nordic countries.[63] This development must therefore be viewed in a Nordic perspective.

Sweden is the Nordic country that has seen the most serious developments in very serious crime in recent years. According to an independent, international organisation doing research on the global prevalence of crime, Sweden ranks *highest* of the Nordic countries in the prevalence of organised and economic crime.[64] In recent years, every police district in Norway has reported varying degrees of presence by members of Swedish criminal networks, in particular related to drug crime. The presence ranges from already established networks to attempts at establishing new or consolidating networks, to individual criminals.

Norway remains an attractive market for drug dealing, as market prices are higher and profit opportunities consequently greater in Norway than in Sweden. The geographic, linguistic and cultural proximity between Norway and Sweden makes it easier for networks to establish themselves and maintain the relations.

In recent years, the police have discovered that several Swedes have committed violence as a service for Norwegian criminal networks. In the coming year, Swedish and Norwegian members of Swedish criminal networks will continue to commit acts of violence and threats in Norway, for themselves or as a service to others. In recent years, the violent crime has taken place in both in private and public space. The violence is mainly triggered by personal conflicts and rivalries over territorial control and control of market shares in the drug trade. Swedish criminal networks have over time built a fearsome reputation for violence, a reputation criminal networks and actors in Norway want to capitalise on.

The illustration is a fictitious representation of organised crime across the Nordic countries.

The past year has seen an emerging trend whereby acts of violence are becoming services bought and sold on digital platforms on the dark web, and increasingly on social media.[65] The police have over time expressed their concern that young Swedes would travel to Norway to carry out violence-as-a-service, a concern emphasised in last year's Threat Assessment. In 2024, this concern was becoming a reality. Criminal networks advertise violent jobs in digital marketplaces, and youths take them on. The violence committed by the youths has changed character. It may be extremely serious and may involve the use of a knife and sometimes guns. The acts of violence also appear more planned and more people are present during the incidents.

"The police have over time expressed their concern that young Swedes would travel to Norway to carry out violence-as-a-service (...) In 2024, this concern was becoming a reality.

For the same period of time, Sweden and Denmark reported a trend whereby youths are enticed with amounts of money in chat groups dedicated to the *"buying and selling"* of acts of violence. The young perpetrators tend not to be gang members themselves or know the victim or the area of the murder. In this way, murder has become a low-status job carried out by hired youths, and organisers seem to make little effort to protect the youth from arrest. The past year's developments in violent crime and the presence of Swedish criminal networks in Norway of course receives a great deal of media attention, and citizens may feel less safe as a result.

There is also increasing cooperation between Nordic actors on other types of crime, and we are registering a development where e.g. drug crime, threats, acts of violence and fraud are interwoven.[66] Fraud finances other crimes, with proceeds being reinvested in e.g. drugs and guns. One example is Nordic criminal actors and networks collaborating on phishing scams across the Nordic countries. The networks operate from e.g. mobile call centres in the Nordic countries and continuously develop new methods for scamming victims.[67] The police are also observing that the threshold for using violence and threats of violence in connection with the crime is lower.

In 2023, frauds increased in all the Nordic countries, resulting in an estimated EUR 826 million in criminal profits.[68] The police are seeing ties between the Nordic actors, also when profits from drug offences and frauds need to be laundered. Profits are used to enable further organised crime, raising the level of violence within and between criminal networks and ultimately the threat to society posed by organised crime in Norway and the Nordic countries.

Photo: The police

USE OF CASH IN NORDIC CRIMINAL NETWORKS

There is reason to believe that a large share of the Nordic cash economy stems from crime and forms part of the criminal economy. Cash is used very little in the Nordic countries compared to the rest of the world. The reason is that the payment services are digitalised. Still, large amounts of cash are in circulation in the Nordic countries, with mostly high-value notes being in demand.[69]

Nordic criminal networks bring cash out of Norway in order to buy large quantities of drugs and launder criminal proceeds. There are several reasons for that. Cash is more commonly used outside the Nordic countries, the anti-laundering system is less rigid, and it creates a distance between the primary crimes and the criminals.[70]

In spring 2023, restrictions were introduced to the receipt in Denmark and Norway of local currency in cash from abroad. The restrictions have made it harder to exchange Norwegian and Danish cash abroad. Danish and Norwegian criminals have therefore been forced to change their modus operandi for transferring assets out of the country and launder criminal proceeds – see page 42, on how criminals convert profits to further crimes.

Criminal networks deliberately recruit vulnerable minors

In recent years, several police districts have seen an increase in minors being recruited by criminals. According to Europol, this recruitment is on the increase in several European countries, with criminals continuously developing new recruitment tactics. Tasks given to minors include selling, transporting and storing drugs. There has also been an increase in minors being tasked with carrying out acts of violence such as extortion, severe violence or murder.[71] Surveys on youths and crime in Norway indicate that it is not uncommon for youths in Norway to know other youths who are employed to commit criminal offences.[72] Recruiting minors to organised crime lowers the detection risk of the organisers and society's chances of prosecution.

Criminal networks employ different methods to recruit and groom youths for crime. They may e.g. be put into debt by receiving money or drugs intended for resale, and then have to "work off their debt" in different ways. Others become members of the network in the hope of easy money, status and excitement. Social media and encrypted communication platforms are frequently used to communicate with the youths. Criminals use different means to glorify a criminal lifestyle and make it appear harmless. Recruitment and grooming of youths for crime are on the rise in neighbourhoods with a high share of vulnerable youths or criminals. Youths with a low threshold for using violence appear particularly at risk of recruitment by criminal networks.[73]

A lack of recognition, perceived social exclusion and discrimination may be important motivators for letting yourself be recruited into gang communities.[74] In Sweden, several of the minors who have taken on violent jobs for payment came from child welfare institutions.[75] The youths may feel it was a voluntary and desired way in, but find it hard to get out again. That may be due to a culture of loyalty in criminal networks, or because they have been threatened or subjected to violence. Some have run up debts which are hard to get out of.[76] Youths employed by criminals do not necessarily identify as victims, but may feel that carrying out criminal offences gives them benefits as members of a community. However, the exploitation of youths — by e.g. taking advantage of their vulnerable position — for your own ends may be a criminal offence, no matter how the situation is perceived by the youths themselves.[77]

Legal goods and services are abused for criminal purposes

The police are seeing that legal services are increasingly being abused by criminals at multiple steps of the criminal process. This is done in connection with e.g. the distribution of drugs to lower the risk of detection, or abuse of trust-based services, to avoid prosecution. The abuse of legal services threaten the things we value in our society, undermining trust in the services affected and a fair justice system.

Carpooling services via apps have gained in popularity in urban areas over the past year. The services give users access to a car when needed without the financial and practical obligations associated with owning a car. These services are, however, increasingly being abused by criminal networks to transport and distribute drugs, a threat expected to continue to increase. It has multiple advantages for criminals. They get access to plenty of cars, and lower the risk of detection by abusing other

THE WAY IN

When he was 11, Noah received gifts and food to keep guard for his elder brother and his friends who were selling drugs for a criminal network. Noah was proud to be included in the community of the older boys. On his mobile phone, Noah's brother showed him cool cars, watches and money in his Instagram account, assets he and his friends had access to by working for the network. At 12, Noah himself received money to store and sell small amounts of drugs and run other errands. As a 15-year-old, he had gained a higher status in the network and had been involved in several violent conflicts.

Drug use, carrying a knife and using violence had become normal parts of everyday life. After a long period of conflict with another criminal network where a close friend of his was stabbed, Noah was getting tired of looking over his shoulder all the time. But he could see no good way out of his criminal lifestyle or other options to achieve status, money and social inclusion.

Noah's story is fictional, but based on several stories from real life.

Police Threat Assessment - Norway 2025 Menu

Illustration of investment passport. Photo: Getty Images

people's BankID (digital identity authentication) data to rent the cars. Another advantage is that people with no driving licence, including minors, can drive the car. BankID data is acquired through illegal means, by threats or fraud, or by people more loosely connected to the networks lending out their personal data voluntarily. Young foreigners employed in passenger transport or by food-delivery services are also exploited by criminals paying to use their employee identities.[78]

Another legal service used for facilitating criminal offences and avoid prosecution is *investment passports*. An investment passport is a citizenship and a new nationality passport issued to private investors for them to inject fresh capital into a country's economy. It is especially used for investment in property complexes. In recent years, several wanted criminals have bought citizenships in countries such as Turkey which have no formal extradition treaties with Norway or other Schengen countries. The police know that a leader of a Swedish criminal network acquired Turkish citizenship through an investment in Turkey. He was issued a genuine investment passport in a false identity after submitting false identity documents in his application. This also illustrates how inadequate controls and security checks in the processing of applications are exploited by criminals to acquire new identities.

Investment passports may give criminals added benefits beyond the avoidance of prosecution in Norway or the Nordic countries. In the coming year, criminal networks will also be able to acquire investment passports for members who are nationals of or have residence permits in *non*-Schengen states, to give them full freedom of movement *inside* Schengen. This they can do because the countries that offer investment passports are generally not subject to a visa requirement for Schengen. Such passports allow network members to move freely inside Schengen and assist networks as intermediaries in everything from arms, drug and cash smuggling to crime-as-a-service, work-related crime, frauds and human trafficking.[79] The investment sums required by the different countries vary, but are generally between NOK 800,000 and 5 million.

There is little transparency by the issuing authorities about the procedures for performing criminal background checks on applicants and establishing the origin of the funds. In several cases, private companies have a role in the government's issuance of investment passports, potentially prioritising the interests of market economy at the cost of necessary security measures, creating a vulnerability for corruption. This, in turn, creates opportunity to launder criminal profits.

Criminals convert their profits into further crimes

Each year, criminal actors and networks make huge profits from crime. To launder their profits, they use both legal financial infrastructures and underground systems for illegal flows of money, often in combination. Profits are not just used for private purposes, but also finances further and more extensive crime. This way, the handling of criminal profits threatens society.

To mitigate the high risk of money laundering, Norwegian banks in spring 2023 introduced restrictions on the repurchase of Norwegian cash from abroad. This has resulted in a large drop in cash declared into Norway, and a rise in the exchange of cash for other assets before they leave Norway. Goods and services are frequently bought to launder profits from drug crime, frauds and work-related crime. Valuable and easily convertible goods whose prices are difficult to set, and hence easy to manipulate, are particularly attractive. Examples of such goods include jewellery, art, collectibles and watches.[80]

There is still a substantial cash economy among criminals, but cryptocurrency is now being used at all levels in the criminal networks operating in Norway. The conversion of cash into cryptocurrency simplifies the financial logistics for them and may become their preferred method of money laundering in the time to come. The development of different cryptocurrencies has enabled criminals to anonymise transactions.[81]

Cryptocurrency is well suited for money laundering, as a cryptocurrency account is cheap and easy to open. This lets them easily and cheaply divide the profits into minor transactions, which makes the laundering more difficult to detect. The greatly fluctuating prices of cryptocurrencies also make it easier to legitimise substantial changes in assets.[82] Despite being associated with high risk, cryptocurrency investments has the potential to grow the criminal profits. Cryptocurrency is used as a means of payment in frauds and ransomware attacks, and to finance criminal activities in Norway and abroad.

It is not uncommon for fraudsters to manipulate victims into converting fiat money into cryptocurrency before sending the cryptocurrency to the criminal's cryptocurrency accounts. There are also examples of criminals taking control of the online bank account of a victim and transferring money to themselves via cryptocurrency exchanges by pretending to be the victim. In many investment fraud cases, the criminals convince victims to let them control their computers via remote control software. In investment fraud, people often pay for a non-existing product or grossly overpay. There are several examples of such frauds. In one police district alone, victims lost NOK 50 million through cryptocurrency investment frauds during the first nine months of 2024.

Police Threat Assessment - Norway 2025 Menu

3.2

CRIME INSIDE THE PUBLIC AND PRIVATE SECTORS

Our society depends on robust public and private sectors where everyone is free to invest, build, develop and administer without having to fear that criminals will erode their income bases and public services. At the same time, criminals, individuals as well as networks, will be highly motivated to take advantage of the finances and expertise in the private and public sectors. The digitisation of society and resulting vulnerabilities amplify the opportunities of criminals to undermine the societal structures we have developed to support the income bases of the private and public sectors.

The exploitation of labour erodes important principles of fairness held in regard in Norway and represents a threat to the things we value in our society. Threats to economic assets and fundamental societal structures endanger a fair labour market and may distort competition in society. This chapter will discuss crime where offenders obtain access to sensitive information which may result in high profits and enable further crime that threatens society.

Photo: Getty Images

Shifting loyalties – risk of criminals recruiting insiders in the financial sector

Employees in banking and finance will in the time to come be at particular risk of bribery, pressure or threats by criminals who want them to perform services for them. Criminals actively look for vulnerabilities in systems and security structures, and are willing to use, and capable of using, people in key roles to facilitate or cover up their criminal activities. These are people referred to as insiders, who in their professional capacity facilitate crime for a third party. The inside activity may be a criminal offence in itself. The insider provides fellow criminals with knowledge of and access to their institution, for them to use for other crimes.

Insiders may facilitate crime deliberately, as a result of pressure or threats, or they may be unaware of it themselves.[83] According to the Norwegian National Security Authority, negative circumstances or perceived unfairness at the workplace may motivate employees to take revenge or harm the institution.[84] One example is down-

sizing, which has occurred in several companies in the finance and telecom sectors over the past year. Corruption and the use of insiders in the public and private sectors are key elements of organised crime and cost them little money.

Several bank employees in Norway are under investigation on suspicion of granting loans on a false basis, leaking sensitive customer information and abusing access to bank systems.[85] The problem is international. In 2023, Europol reported that 60% of criminal networks in Europe resort to corruption to attain their goals.[86] Studies in Sweden show that organised criminals work systematically to recruit insiders in banking.

One of the reasons why bank employee are especially attractive targets for criminals is that banks have improved their cyber security and systems for detecting suspicious transactions, making money-laundering transactions easier to discover. Using insiders also conceals the criminals' link to the offence.

Criminals make high profits from stealing sensitive information

In a globalised and digitised world, knowledge is often what gives a business its competitive edge. Criminals try to take advantage of that, as unauthorised access to other people's sensitive information may generate high profits. They can sell the information to others or blackmail its owner to avoid resale. Businesses that operate in extremely competitive markets and businesses that store the personal data of their customers will be particularly vulnerable to this type of cybercrime.

Cybercrime has long been a threat to businesses. That has driven them to invest heavily in cyber security systems, including back-ups of sensitive information. This has had a positive effect, but several criminals have now changed their MO. Before, criminals were very successful in encrypting corporate data, locking employees out of their own files and demanding ransom to decrypt the data. Now, businesses are to some extent immune to this threat because they have started storing the information in multiple locations with different security levels. Some cybercriminals have consequently changed tactics, opting to blackmail victims without locking and encrypting corporate computer systems. They do this by intruding into computer systems and stealing sensitive information, which they then threaten to sell or publish unless the victim pays ransom.

The combination of stolen data and publicly available information may threaten both individuals and national security interests. This situation is getting worse as criminals start using new technology, such as artificial intelligence, which enables even more precise and targeted cybercrime.

> *The combination of stolen data and publicly available information may threaten both individuals and national security interests.*

Police Threat Assessment - Norway 2025 Menu

Cyber attacks on small and medium-sized businesses can have serious consequences

Profit-motivated criminals still dominate in cybercrime, frequently using ransomware. Alongside data thefts, ransomware attacks pose a substantial and growing cybercriminal threat to Norwegian businesses and their contractor chains. The police know of victims throughout Norway and in all police districts over the past year, with levels of under-reporting believed to be high. Microsoft reports a near tripling of ransomware attacks globally in 2024.[87] National borders are no obstacle in this context. Small and medium-sized businesses are especially at risk, as they are generally more vulnerable and less equipped to handle the consequences of such malware attacks. These businesses may be important contractors or sub-contractors of enterprises or services which control critical infrastructure and support vital national functions.[88]

Over the past year, the police have observed attacks on different parts of enterprise value chains and on third-party partners. Cyber-dependent value-chain attacks happen when someone without authorisation adds properties to, or modifies parts of, a product for future exploitation. Such modification may take place in every part of the value chain, via software, hardware or system documentation. Value-chain attacks target products under development, whereas third-party attacks are perpetrated against contractors or subcontractors to affect multiple enterprises or services.

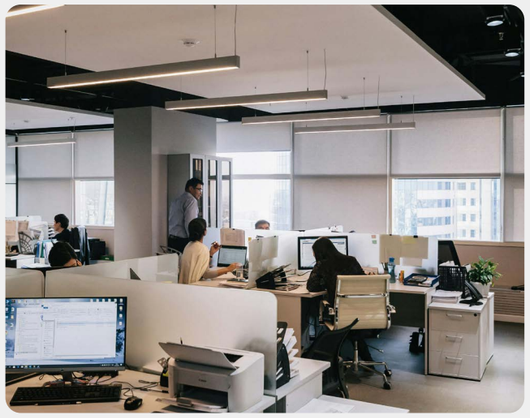


Photo: Unsplash

Long and complex contractor chains represent a vulnerability exploited by threat actors. Serious disruption of ICT systems may, in the worst-case scenario, threaten economic stability and impact public safety and security.[89] Cyber criminals' threats to contractor chains and small and medium-sized businesses in Norway are expected to become more precise. The level of harm is also expected to increase, as are the challenges involved in safeguarding critical assets and services. Attacks via third parties are expected to continue to rise, as many enterprises have systems that are integrated with those of subcontractors or other partners and thus vulnerable to attack and exploitation by the threat actors.

> *The increased digitisation of society means that such systems are connected to the internet and hence vulnerable to cyber attacks, including with ransomware.*

A number of enterprises and services that are vital to society also control physical processes in water supply and sewage, energy supply etc. They use so-called operational technology, often older computer systems that were built to be robust and reliable but lack important security features, as they used to be off line. But the digitisation of society means that Norwegian operational technology has become connected to the internet, too, and hence become vulnerable to cyber attacks, including with ransomware, Attacks on these systems may entail loss of production and downtime or wide-reaching security challenges for e.g. critical infrastructure and societal functions.

Government database crime drains public funds

Government database crime is a threat that is expected to rise in the time to come. This is a type of fraud where data used for verification of individuals, enterprises and master data is manipulated in digital systems.[90] The police are observing that government database crime has received more attention from known criminal networks in Norway and abroad. It threatens society, as it has substantial economic implications for society and potentially serious negative implications for individuals who are victims or exploited.

In government database crime, criminals deliberately report false or fictitious master data to the authorities, data on which the verification of the identities of persons or companies is based. This manipulated data is then used to verify decisions, including in public administration, which generate profits for the criminals. The crime is often carried out in a systematic collaboration between multiple parties and may soon have great dimensions. The manipulation of data is carried out by criminals to access all types of payments, financial support and refunds, from companies as well as public authorities. Public funds are deprived of money through tax evasion, wrongful VAT refunds and benefit fraud. In the finance sector, loan frauds cause loss of income and high losses.

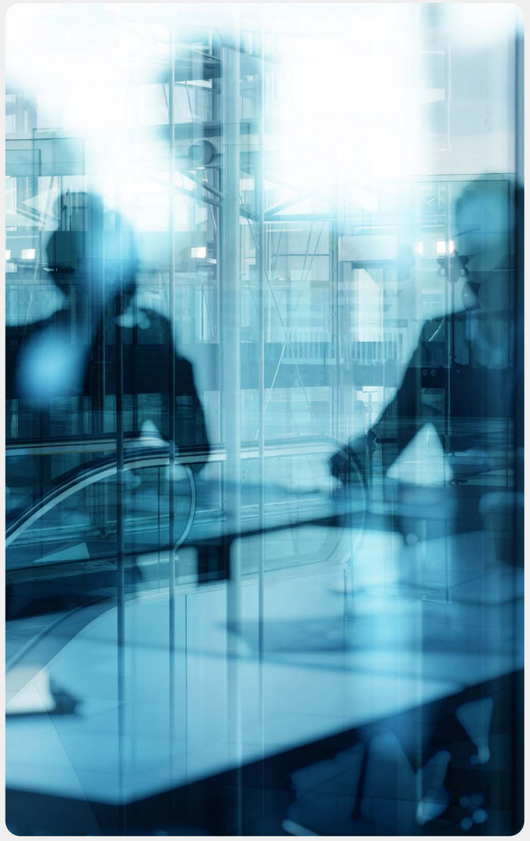


Photo: Getty Images

AUTHENTIC EXAMPLE OF GOVERNMENT DATABASE CRIME THAT THREATENS SOCIETY

A number of companies were created online in the government databases at Brønnøysund Register Centre with the stated purpose of running grocery shops. The persons holding roles in the companies were used as fronts.

The companies submitted false VAT returns over several years, leading to NOK 1.5 million of evaded VAT. Furthermore, the account-keeping breached the Accounting Act and the Bookkeeping Act, e.g. by neglecting to enter earnings in the accounts and by providing inadequate evidence of earnings and costs.

The identities of fronts were used to apply for and receive a licence to sell alcohol. The beneficial owner would not have been granted a licence in his own name.

He submitted information about employees and reported income for fictitious employees. In addition, he underreported the hours worked by several people, who could then claim work-assessment allowances and unemployment benefits. The Norwegian Labour and Welfare Administration paid more than NOK 1 million to persons who were not eligible for financial support.

The defendant was convicted of aggravated fraud, contribution to aggravated fraud and making a false statement by manipulating information in government databases, and sentenced to 2 years and 9 months in prison.

Photo: Getty Images

The prevalence of government database manipulation and associated economic crime is unknown. But known case complexes show that it involves a large number of people, who are left with high profits. The government agencies affected by database manipulation refer to high numbers of undetected cases. Estimates suggest it generates billions of NOK in criminal profits.

A number of vulnerabilities make database manipulation possible. When services are going to be digitised, risk assessments lack a broader societal perspective and the potential for manipulation and crime are not sufficiently taken into account. Increased user friendliness and simplifications have also made it easier for criminals to manipulate and abuse the systems of the welfare state. The sharing of information between government departments is lacking, and the potential for a more automated and structured sharing of suspicions of manipulation has not been explored.

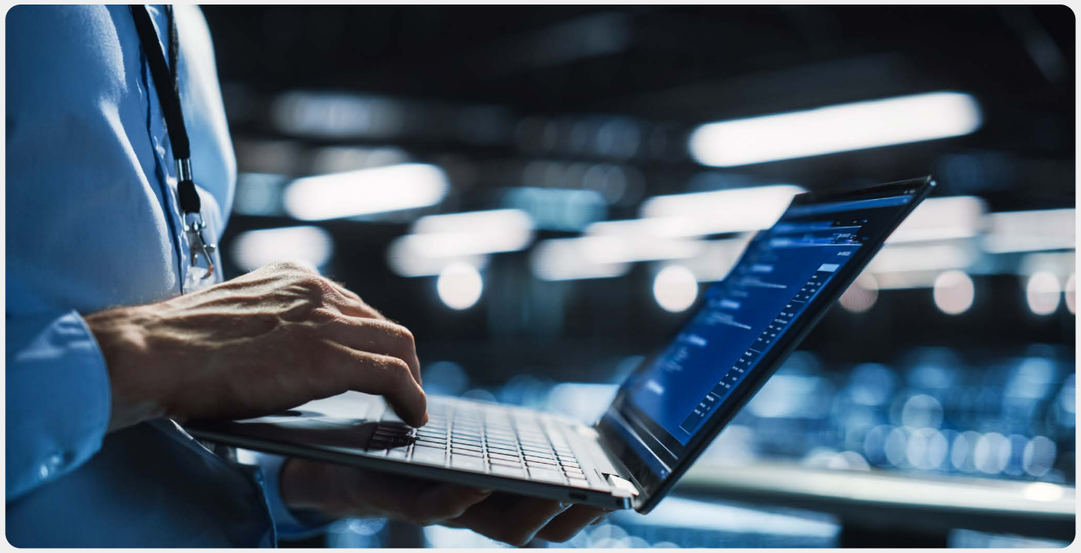


Photo: Getty Images

3.3

CRIMINALS ABUSING TECHNOLOGY AND TRUST

Children in Norway spend a lot of time online on digital platforms, where the technological advances in areas such as anonymisation and artificial intelligence make it easier for criminals to seek sexual contact with minors. That makes Norwegian children vulnerable to sexual abuse and constitutes a major threat to the digital safety of children and teenagers. Children and teenagers are vital to the future of our society and deserve special attention and protection. What threatens the safety of our children and teenagers in general thus threatens society directly.

Some of the children tricked into sexual contact online are in a particularly vulnerable position. Some have a history of being physically or sexually abused, and suffer from physical or emotional ill-health. Others have difficult circumstances at home, such as alcohol or drug abuse by parents, are in the care of the Child Welfare Service or live in an institution. Children in a vulnerable position have a higher risk of being sexually exploited online. They have a greater tendency to seek the care of adults for a sense of belonging and recognition, a reliance cynically taken advantage of by predators. Victims of physical or sexual abuse run a higher risk of being abused again. Children in vulnerable positions tend to have fewer people to lean on when they have been exploited.[91] More girls than boys are contacted by predators.[92]

Convicted sexual offenders exploit children who sell self-generated sexual material

In recent years, there have been an increasing number of reports of children selling self-generated material to adults on digital platforms, predominantly Snapchat. This is sexual material where children have filmed or photographed themselves. Some of the buyers are convicted sexual offenders who pose a particularly high threat to the children.

A survey conducted by the Norwegian Media Authority shows that as much as 26% of children aged 9–11, and 84% of children aged 12–14, use Snapchat, despite the platform's age limit of 13 years.[93] In many cases, the children themselves contact the buyers of self-generated sexual material on social media. Other children may also facilitate contact, or the offender initiates it. In the latter case, children who originally had no desire to sell material may end up doing so because the opportunity presents itself or they are manipulated or pressured.

Children who start selling self-generated material to strangers run a greater risk of ending up in situations where they are enticed or pressured into selling more material, or meeting the buyer in real life to sell sexual services. Many of the buyers have a history of sexual abuse of children or other serious offences. They therefore pose a huge threat to children they come into contact with.

The self-generated material sold will in many cases be shared among people taking a sexual interest in children. In recent years, the police have noted that a great deal of new sexual abuse material is self-generated.

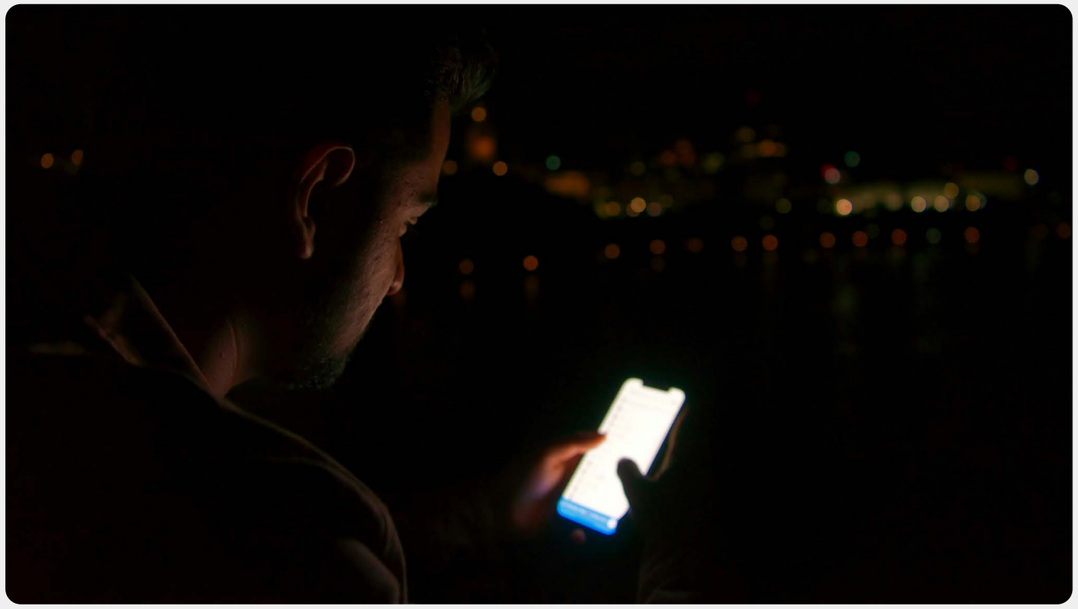


Photo: Unsplash

The children's motivation for selling the material is mainly money. As most victims do it voluntarily, they do not report the incidents to the police themselves. Some cases are reported by parents who have noticed that the child has received money from someone unknown, while other sales are detected by the payment services used. Buyers pay through different digital payment services, mainly Vipps, who extended their instant payment service to all the Nordic countries in 2024.[94] Services offering instant international payments may widen the opportunities for Norwegian children selling self-generated material, raising their risk of being subjected to digital or hands-on sexual abuse.

Irrespective of children's motivation, it is still illegal to acquire sexual material showing minors or to buy sexual services from them.

EASY MONEY AT WHAT COST?

"Nina" felt she had less money than her friends and was looking for an easy way to get more. She therefore actively sought out unknown men on Snapchat. When chatting with the strangers, Nina told them she was a minor. This did not deter the men. Having established contact with several men, she started selling images of herself. She received different amounts for pictures she sent of different parts of her body. This went on for a while, but then Nina's parents discovered that a stranger had transferred money to their daughter's account via e.g. Vipps. The case was reported to the police.

Nina's story is a fictitious story based on many stories from real life.

Photo: The police

Profit-motivated criminals use artificial intelligence to pressure minors

The police note that the volume and quality of synthetic child sexual abuse images is rising. This development indicates that in the near future, we will see synthetic child sexual abuse videos of realistic quality. Criminals use artificial intelligence both to generate new synthetic child sexual abuse material and to modify older material. The material is shared on the dark and open webs.

Synthetic child sexual abuse material is an umbrella term denoting all kinds of material (photos, videos, text etc.) that shows child sexual abuse or otherwise presents children in a sexual way, generated using generative artificial intelligence.

Synthetic child sexual abuse material has multiple negative consequences. Firstly, the generation of such synthetic material may lead to real children being depicted, even though they are not victims of sexual abuse. In theory, all children in photos or videos posted on e.g. social media may be depicted in synthetic child sexual abuse material, as it can be generated from innocent photos or videos. Secondly, it may become difficult to distinguish synthetic from real child sexual abuse material, and so the police may waste their time trying to identify non-existent children, while real child sexual abuse material may appear synthetic. In Norway, all kinds of sexual representations of children are prohibited, irrespective of how it was made. But as evidence of sexual abuse, the synthetic material will challenge the police, prosecuting authority and courts in the time to come.

Although the police have seen several cases of extortion using synthetic nude images over the past year, real photos and videos of the victim are still used in the majority of cases. The advances of artificial intelligence make financially motivated sexual extortion easier to commit. Artificial intelligence may for instance be used to generate synthetic nude images of victims, so that blackmailers no longer need to trick them into sharing nude images of themselves for the purpose of extortion. In addition, artificial intelligence may be used for selecting promising victims in a more efficient and precise manner.

The police note that blackmailers tend to be more cynical and aggressive than they used to be. Translation tools e.g. let them adapt their language and jargon to the individual child victim. There is some cooperation between actors, who operate from different countries. Blackmailers frequently operate from the Philippines, Nigeria and the Ivory Coast.

The vast majority of victims of financially motivated sexual extortion are boys and men. Most victims are adults aged 18-30, while about one sixth are minors down to as young as 10. Such extortion can put a huge strain on victims, financially as well as emotionally. If the victim pays once, there is a high chance of the blackmailer demanding more money from him. So many victims end up paying multiple times. The police know that Norwegian victims have paid about NOK 7.6 million to blackmailers around the world since January of 2023. In several countries, including Norway, victims of sexual extortion have been driven to suicide.

> *In several countries, including Norway, victims of sexual extortion have been driven to suicide.*

3.4

CRIME AGAINST THE ENVIRONMENT AND THE COMMUNITY

The police also define threats to nature, the environment and animal welfare as crime which threatens society. Such crimes diminish our shared assets, as they weaken the very foundations of our livelihood – nature, an abundant wildlife and the future of coming generations – but also because of their present seriously detrimental effect on the economy. The international trend is for criminal networks to also commit organised crime that harms the environment. Profits made from environmental crime finance further serious and organised crime.[95]

Both Interpol and Europol highlight the fight against environmental crime as being central to the efforts against serious and organised crime.[96,97] Environmental crime is estimated to be the internationally third most profitable type of organised crime, after drug and forgery offences, such as the sale and use of counterfeit goods, identity documents or currency. No national borders protect against environmental crime and it affects us all. Crime within and associated with the aquaculture industry hits Norway especially hard because the industry is pivotal to Norway's economy and international reputation. This chapter will focus on fisheries crime, illegal export of production fish, and organised and illegal trade in endangered species, which is detrimental to biodiversity.

Misreporting of catches causes high economic losses

In Norway, all catches of fish must be landed and reported, except for viable fish caught contrary to regulations. These must be released back into the sea immediately. However, the landing regulations are not fully complied with. This seems to be a widespread problem that is not limited to one type of actor, fishery or fleet group. The criminal opportunities are ample, and the threat is expected to increase in scale and severity. The crime threatens society because it deprives the state of income and threatens the sustainable management of the fish stocks that form part of our livelihood.

Mis- and under-reporting of catches may take many forms and constitute different offences. Some examples are so-called high-grading of catches or other breaches of the landing requirement. High-grading is landing the best parts of the catch only, while sorting out smaller fish or shellfish and throwing them back into the sea without reporting it. Whole catches may also be thrown back into the sea, including dead or dying individuals.

> *Environmental crime is the internationally third most profitable type of organised crime.*

Other examples of mis- and under-reporting is when plants omit to record whole or parts of landed catches, or record catches as different species. The latter is often to circumvent quota regulations, and the fisherman and plant may agree to do it that way.

The threat includes illegal catching of red king crab, and under-reporting of legal catches. The king crab is not considered native to Norwegian fauna, but the policy has still been to conserve a quota-regulated population in a limited area east of North Cape. In 2023, 2110 tons of king crab worth NOK 704.3 million was harvested.[98] The high market prices attained for king crab motivate actors to catch it illegally and make good money from it. The police note that the actors are not only individuals such as recreational fishermen, but also criminal networks engaging in systematic illegal harvesting and misreporting.

Illegally caught king crab is also sold illegally, often along the transport routes used for legal exportation. Norway has a number of unguarded border crossing points that lend themselves to the smuggling of king crab. The lone actors sell smaller quantities on digital market platforms and social media. These shipments are often paid cash and distributed to restaurants and private individuals nation-wide.

Mis- or under-reported catches are camouflaged and moved on through irregular sales, transport and export. This type of crime may skew fish stock figures, figures used for calculating future quotas, and may so, in the worst-case scenario, harm the sustainability of fisheries.

Poor animal welfare and illegal fish exports threaten our common value creation

Aquaculture is Norway's second largest export industry, after gas and oil. Value creation by this industry is consequently vital to the Norwegian economy and serious crime in this sector may pose a direct threat to society. As in farming on land, the goal is for farm fish to be treated well, but there are considerable problems with animal welfare in the aquaculture industry. In 2024, 57.8 million farm salmon died in the sea phase, a mortality rate of 15.4%. This was slightly down from the peak year of 2023, where the mortality rate was 16.7%.[99]

Photo: Getty Images

The fish-farming industry consists of various operators and includes companies operating net pens, smolt producers, bleed vessels and harvesting plants. The fish reared in Norway is predominantly Atlantic salmon, rainbow trout and Arctic char. The high mortality in net pens is mainly due to infections that easily spread in crowded environments, injuries sustained through delousing operations, *Moritella viscosa* lesions and growth of algae.[100] In some cases, large numbers must be slaughtered for animal welfare reasons.

Farm fish with lesions, deformities, signs of serious mis-handling or other quality defects will often not survive ordinary transport to harvesting plants. Emergency slaughter is performed in such instances. The police know that large amounts of fish are treated poorly and illegally during emergency slaughter so that it does not die immediately and has to suffer in this phase, too. Emergency-slaughtered fish is sorted as production fish.

While not dangerous to eat, production fish cannot be sold for human consumption before the defects have been corrected through processing. That may be to cut off parts not fit for consumption, e.g. lesions or discolouration. It is illegal to export production fish without correcting defects in Norway first. The guidelines for the export of production fish are designed to protect the reputation of Norwegian salmon in the international market, ensure traceability and food safety for consumers.

At times, there is a high share of production fish in the market. This may be a driver of the sale and illegal export of production fish. Shipments of Norwegian farmed salmon with deep wounds, discolouration and a milky, sticky slime have been discovered abroad, shipments destined for the human consumption market. Illegal export of production fish may generate high profits, but because the practice is intertwined with legal activity, it is difficult to quantify its share of total profits.

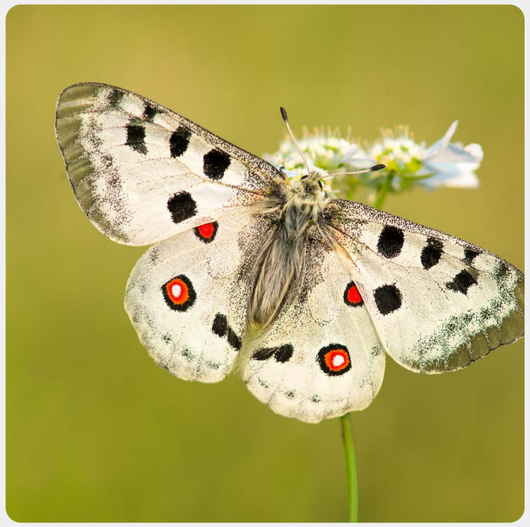
Illegal trade in endangered species reduces biodiversity

Illegal harvesting of and trade in endangered species of wildlife and plants constitute a persistent threat to bio-diversity in Norway and internationally. Though less visible to the public eye, this type of crime is definitely harmful to society. Global climate changes threaten biodiversity, both flora and fauna. That may lead to a rise in illegal trade in endangered, rare species and their products. The more endangered and rare the species, the higher its market value. Norway has its place among the players in this market, as an importer and a supplier.

We are primarily an importing country in this context. Norwegian players illegally import endangered species for commercial distribution and as private collectors. According to Customs, the illegal import of birds and reptiles is a pertinent example, some of which must be considered organised crime and involves e.g. the forgery of permits. The offences coincide with drug smuggling and trade in other illegal goods.

As a supplying country, what mainly attracts both Norwegian and international criminal actors and networks is Norway's abundant and diverse bird fauna. In 2023, the police seized 53,000 eggs from endangered bird species in one of the most serious cases of fauna crime seen in Norway so far. The Illegal harvesting of eggs from endangered bird species in Norway takes place in the context of an international market for illegal harvesting of and trade in eggs, and harms biodiversity because it is a factor in driving species to the brink of extinction.

The traders in this illegal market have different intentions. Many are unaware of what they are part of, some are private collectors, while others are professional, profit-motivated criminal actors. For criminal networks, there is a great potential for illegal profit, as some species command extremely high prices in the illegal market.



The Apollo butterfly is on the Red List and near threatened in Norway. Photo: Getty Images

3.5

CRIME IN UNCERTAIN TIMES

We live in a world where conflicts are flaring up again along ever more ideological lines. In the international arena, the level of cooperation and mutuality has been reduced, with interactions between states being dominated by super-power rivalries. In parallel, voters and the political discourse have moved in a more nationalist direction world-wide. In Norway, too, there are hard-line attitudes and heated debates. This backdrop, combined with exponential techno-logical developments, may present some challenges to Norwegian fundamental societal structures, including vital democratic principles and processes.

Uncertain times are not just about differences of opinion. The coming year will continue to be defined by armed conflict in many regions. The associated regional instability and other coinciding forces are likely to sustain the heavy migratory pressure on the EU and Norway. Over the years, this has created a large market for people smuggling, where organised criminals motivated by profit will, also in the year to come, have ample opportunities to take advantage of migrants.

> *It may be demanding. But a society in which we only talk to people who are similar to ourselves will be a poorer and more dangerous one.*
>
> **The King's New Year Speech, 2024**[101]

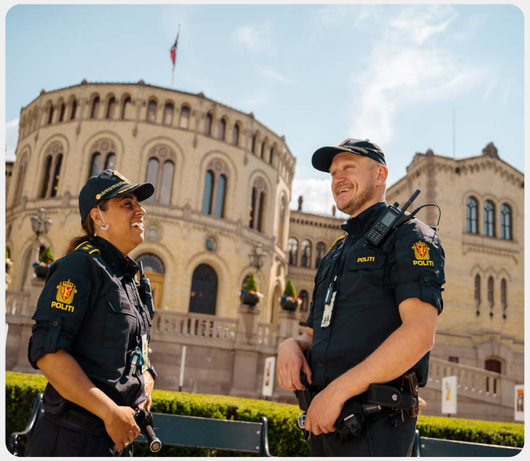


Photo: The police

Democratic processes will be under pressure in the election year of 2025

A vital part of a free and well-functioning democracy is the freedom to speak and take part in debates, physically and digitally. This is especially important in Norway in 2025, a year of general and Sami parliamentary elections. Society relies on the free and unfiltered expressions of opinion by those who perceive injustice or want a shift in political priorities. That being said, there is a point where statements overstep the mark and become criminal. Some of these statements constitute threats to demo-cracy because they prevent others from participating in public debate. The developments in hate crime and potential use of hybrid means give reason to be particularly alert to threats which may interfere with democratic processes in the year to come.

Indications are that Norwegian politicians are increasingly subjected to hate speech, mainly on social media.[102] With social media, far more people are able to express their opinions and take part in public debate than before, but they have also contributed to more unfiltered attacks on someone's character, harassment and conspiracy theories. Central platforms and companies such as X (formerly Twitter) and Meta have already scaled down their moderation of potentially threatening or hateful content, or are planning to do so. Democratically elected politicians must tolerate a certain level of criticism in their roles, but many find the high level of hate speech demanding. The consequence is that many are reluctant to participate in public debate and some step down from office. A survey shows that more than 40% of democratically elected politicians who had such experiences chose to change their behaviour, e.g. in the form of self-moderation.[103]

Many participants in democracy are met with harsh attacks also outside the political sphere. Hate speech or other hate-motivated crime targeting vulnerable and exposed social groups are particularly likely to scare their representatives into silence.

Democratic processes may also be interfered with through the use of hybrid means to exert malign influence. Recent years have seen numerous examples of inter-ference in elections in the Western world.[104] US author-ities recently disclosed that they had detected a high volume of attempts by state actors to interfere in the 2024 presidential elections. A number of the confirmed cases were attempts to give the impression of ongoing electoral fraud.[105] Given the fast-paced development of artificial intelligence, such influence operations may increase exponentially. It will be demanding to distinguish between information and disinformation, and legal and illegal activity. Malign influence activity through the dissemination of disinformation will in many cases fall within the remit of the general police force.

> «*States are also growing more sophisticated in digital influence operations that try to affect foreign publics' views, sway voters' perspectives, shift policies, and create social and political upheaval. Digital technologies have become a core component of many governments' repressive toolkits*»
>
> **U.S. Office of the Director of National Intelligence, Annual Threat Assessment, 2024**[106]

Politically motivated criminals may pose a threat to societal functions

Not all malign disruption of fundamental functions through sophisticated digital means is carried out by representatives of a foreign state, not by far. Politically motivated cybercriminals are activists who commit crime motivated by political opinion or conviction. Their actions are known as *hacktivism*, and are traditionally associated with various forms of denial of service attacks. These criminal actors pose a threat to fundamental societal structures by trying to get their political message across through undemocratic means.

The organisation of such actors is typically very fluid, with individuals and groups collaborating transnationally on different projects. Some may also, consciously or unconsciously, carry out criminal activity on behalf of a state actor. Determining the underlying motivation of hacktivists can be very demanding.

They fight for a variety of causes. In recent years, security policy conflicts have been a frequent source of hacktivism. More collaboration between different hacktivist groups appears to have expanded their available toolkit and enabled them to carry out more complex cyber attacks with a higher potential for harm.

> *More collaboration between different hacktivist groups appears to have expanded their available toolkit and enabled them to carry out more complex cyber attacks with a higher potential for harm.*

The Holy League is one example of a hacktivist group united by their shared anti-Western, anti-Israeli and pro-Russian attitudes. Despite their differing approaches and partially differing ambitions, the groups share knowledge with each other and cross-collaborate to achieve different effects.[107]

The developments in 2024 show that hacktivists are flexible in their methods of operation, and that cyber-criminals go further and further in their use of means to achieve their goals. Besides more classical denial-of service attacks, several hacktivist groups now also use malware to commit politically motivated ransomware attacks internationally. Hacktivists and profit-motivated cybercriminals have directly and indirectly affected operational technology to support their objectives.[108,109]

Ransomware attacks motivated by ideology or political causes rather than profit have yet to reach Norway. But given the international developments, there is still a growing danger that this or other cyber activism will disrupt processes, functions or democratic institutions in Norwegian society.[110,111,112]

Conflicts in the Middle East will boost the market for people smuggling services

In 2024, more than 50% of asylum seekers who arrived in Norway were assisted by people smugglers on their journey. This does not include Ukrainian nationals or others with ties to Ukraine, who have applied for collective protection. The majority of those that used people smugglers to reach Norway crossed the Greek border from Turkey and are migrants from the Middle East who took the sea or overland route. From Greece, criminal networks facilitate their onward journey on false documents by air to other European countries, including Norway. The people smugglers charge

Migrants being rescued in the Mediterranean. Photo: The police

thousands of euros for the journey from Turkey to Norway. The worsening of conflicts in the Middle East in 2024 will be a push factor for migration and boost demand for people smuggling services.

Norwegian criminals cooperate with transnational people-smuggling networks operating in Norway and abroad. The majority of people smuggled to Norway are, however, assisted by foreign criminals who live abroad. In many cases, the smugglers come from the same countries as the migrants or from the countries along the different smuggling routes.

The networks operate across wide areas, from the migrants' country of origin to transit and destination countries, facilitating services such as transport, false documents and accommodation throughout the journey. They remotely control the migrants via encrypted communication and map applications, guiding them on where to cross national borders illegally. Social media and platforms are also used to promote smuggling services.

In general, the services are paid for via agencies, with the payment only becoming available to the smugglers when the migrant has reached the country of destination. Some smugglers use a pay-as-you-go approach, demanding payment for each leg of the journey. Reports of people smugglers using violence against migrant are increasing.

People smuggling is associated with serious human rights violations and deaths and are among the most serious forms of crime faced by Europe. More than 2200 migrants were reported dead or missing in 2024 after attempting to cross the Mediterranean. The type of crime is associated with abuse of identity documents, human trafficking and other serious crimes. People smuggling is profitable for the criminal networks, with estimated annual earnings of several billion euros worldwide. To maximise their profits, smugglers put migrants in increasingly dangerous situations.

REFERENCES

1. NDLA. 2024. PESTEL. Source: https://ndla.no/nb/r/markedsforing-og-ledelse-2/pestel---ekstern-analyse/a6cc8b59e9
2. Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim). 2024b. *Økokrim threat assessment 2024 – The criminal economy.* Source: https://img8.custompublish.com/getfile.php/5363097.2528.ajtsilqbikkmsk/2024_Trusselvurdering_%C3%98kokrim_nett.pdf?return=www.okokrim.no
3. Prime Minister's Office. 2025. *The Prime Minister's New Year Speech 2025*. Source: https://www.regjeringen.no/no/aktuelt/statsministerens-nyttarstale-2025/id3081460/
4. Norwegian Intelligence Service. 2025a. *Fokus 2025.* Source: https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-pa-norsk/Fokus2025%20-%20N0%20-%20Weboppslag%20v4.pdf/_/attachment/inline/23849b35-548a-4f8b-a1fc-a30f4a7d6b77:62422850e2c371d06db67622dbf2c09ae678264d/Fokus2025%20-%20N0%20-%20Weboppslag%20v4.pdf
5. Norwegian Intelligence Service. 2025a.
6. Police Security Service. 2025. *National threat assessment 2025*. Source: https://pst.no/globalassets/2025/nasjonal-trusselvurdering-2025/nasjonal-trusselvurdering-2025_no_web.pdf
7. Malerud, S., Hennum, A.C. & Toverød, N. 2021. *Situasjonsforståelse ved sammensatte trusler – et konseptgrunnlag.* FFI-rapport 21/00246. Source: *https://www.ffi.no/publikasjoner/arkiv/scenarioer-for-uonsket-pavirkning-i-forbindelse-med-norske-valg*
8. Ministry of Digitalisation and Public Governance. 2024. *Fremtidens digitale Norge. Nasjonal digitaliseringsstrategi 2024–2030.* Source: https://www.regjeringen.no/contentassets/c499c3b6c93740bd989c43d886f65924/no/pdfs/nasjonal-digitaliseringsstrategi_ny.pdf
9. Norwegian Board of Technology. 2024a. *Teknotrender for Stortinget 2024*. Source: https://teknologiradet.no/publication/teknotrender-for-stortinget-2024/
10. National Criminal Investigation Service. 2023. *Etterretningsrapport: Generativ Kunstig Intelligens*. Source: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/etterretningsrapport-generativ-kunstig-intelligens-kripos.pdf
11. Future Investment Initiative Institute. 2024. *Elon Musk and Dr. Peter Diamandis #FII8 Conversation on the Future of #AI.* Source: https://www.youtube.com/watch?v=3JkkWfzc4Jg
12. Norwegian police. 2023. *DELE=DELTA: Om deling av voldsvideoer.* Source: https://www.politiet.no/rad/trygg-nettbruk/deling-av-voldsvideoer/#mange-vet-ikke-hvor-grensene-gaar---slik-er-loven, https://www.politiet.no/globalassets/tall-og-fakta/voldtekt-og-seksuallovbrudd/fenomenrapport-exposed-kontoer.pdf
13. European Consortium for Political Research. 2024. *Dimensions of polarization, realignment and electoral participation in Europe: The mobilizing power of the cultural dimension.* Source: https://ejpr.onlinelibrary.wiley.com/doi/full/10.1111/1475-6765.12718?campaign=wolearlyview
14. Pew Research Center. 2024. *Political Polarization in the American Public How Increasing Ideological Uniformity and Partisan Antipathy Affect Politics, Compromise and Everyday Life*. Source: https://www.pewresearch.org/politics/2014/06/12/political-polarization-in-the-american-public/
15. Politico. 2024. *Europe's growing polarization spells trouble*. Source: https://www.politico.eu/newsletter/politico-confidential/europes-growing-polarization-spells-trouble/
16. Gripsrud, Jostein. 2023. *Polarisering: Et historisk blikk på norsk politikk og offentlighet*. Source: https://www.idunn.no/doi/10.18261/tfs.64.3.9#sec-7
17. Norwegian Board of Technology. 2024a.
18. Statistics Norway. 2024. *Fattigdomsproblemer, levekårsundersøkelsen.* Source: https://www.ssb.no/sosiale-forhold-og-kriminalitet/levekar/statistikk/fattigdomsproblemer-levekarsundersokelsen
19. Institute of Health Equity. 2023. *Rapid review of inequalities and wellbeing in Norway since 2014.* Source: www.instituteofhealthequity.org
20. Ministry of Justice and Public Security. 2024a. *Felles verdier – felles ansvar. Meld.St.15. (2023-2024).* Source: https://www.regjeringen.no/no/dokumenter/meld.-st.-15-20232024/id3031227/?ch=1
21. Directorate for Children, Youth and Family Affairs. 2023. *Fattigdom - veileder om arbeid for barn som lever i fattige familier.* Source: https://www.bufdir.no/fagstotte/produkter/veileder-fattigdom/
22. NOVA. 2018. *Muligheter og hindringer for barn i lavinntektsfamilier. En kunnskapsoppsummering.* Source: https://www.nhri.no/wp-content/uploads/2019/01/Rapport-fra-NOVA-Muligheter-og-hindringer-for-barn-i-lavinntektsfamilier-2018.pdf
23. Norwegian Institute for Nature Research. 2015. *Klimaendringenes påvirkning på naturmangfoldet i Norge.* NINA Rapport 1210. Source: https://www.miljodirektoratet.no/globalassets/publikasjoner/M443/M443.pdf
24. Lovdata. 2021. *Kapittel 3. Vergemål for mindreårige. § 8. Mindreårige*. Source: https://lovdata.no/nav/lov/2010-03-26-9/kap3/%C2%A78
25. National Criminal Investigation Service. 2025a. *Narkotika- og dopingstatistikk 2024.* Source: https://www.politiet.no/globalassets/tall-og-fakta/narkotika/narkotikastatistikk-2024.pdf
26. National Criminal Investigation Service. 2025a.
27. Customs Service 2025. *Rekordmengder marihuana beslaglagt i 2024: – Vi ser en tydelig trend*. Source: https://www.toll.no/no/om-tolletaten/aktuelt-fra-tolletaten/rekordstore-mengder-beslaglagt-i-2024
28. NOVA & Oslo Met. 2024a. *Ungdata 2024. Nasjonale resultater*. Source: https://oda.oslomet.no/oda-xmlui/handle/11250/3145138
29. Oslo University Hospital. 2024a. *Ekspertsykehuset – OUS sin blogg for fag, forskning og innovasjon. Kokainrus – til en pris du ikke ønsker å betale.* Source: https://www.oslo-universitetssykehus.no/om-oss/ekspertsykehuset/kokainrus---til-en-pris-du-ikke-onsker-betale/
30. NOVA & Oslo Met. 2024a.
31. Oslo University Hospital. 2024a.
32. National Criminal Investigation Service. 2025a.
33. Global Initiative Against Transnational Organized Crime. 2024. *European drug trends monitor*. Source: https://globalinitiative.net/wp-content/uploads/2023/09/Global-organized-crime-index-2023-web-compressed-compressed.pdf
34. National Criminal Investigation Service. 2025a.
35. Oslo University Hospital. 2024. *Bekymringsfull økning av nitazen-relaterte dødsfall*. Source: https://www.oslo-universitetssykehus.no/om-oss/nyheter/bekymringsfull-okning-av-nitazen-relaterte-dodsfall/
36. Norwegian Institute of Public Health. 2023. *Dødsårsaksregisteret*. Source: https://www.fhi.no/op/dodsarsaksregisteret/

Police Threat Assessment 2025 Menu References

37. Norwegian Institute of Public Health. 2024. *Høyeste antallet narkotikautløste dødsfall siden 2001*. Source: https://www.fhi.no/nyheter/2024/hoyeste-antallet-narkotikautloste-dodsfall-siden-2001/
38. National Criminal Investigation Service. 2025a.
39. Store norske leksikon. 2022. *Voldslovbrudd.* Source: https://snl.no/voldslovbrudd
40. National Criminal Investigation Service. 2025b. *Drap i Norge 2014-2024 – Nasjonal drapsoversikt. https://www.politiet.no/globalassets/tall-og-fakta/drap/nasjonal-drapsoversikt-2024.pdf*
41. National Criminal Investigation Service. 2025b.
42. Oslo municipality. 2023. *SaLTo-rapporten: Barne- og ungdomskriminaliteten i Oslo. Rapport basert på data fra 2023*. Source: https://www.politiet.no/globalassets/dokumenter-strategier-og-horinger/oslo/rapporter/barne--og-ungdomskriminalitet/salto-rapporten-2023.pdf
43. Ministry of Justice and Public Security. 2024a.
44. Europol. 2024a. *Decoding the EU's most Threathening Criminal Networks.* Source: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20report%20on%20Decoding%20the%20EU-s%20most%20threatening%20criminal%20networks.pdf
45. Store norske leksikon. 2024. *Vinningslovbrudd.* Source: https://snl.no/vinningslovbrudd
46. Norwegian Broadcasting Corporation (NRK). 2024. *Nye tall for ungdomskriminalitet. Økning i antall ran og voldshendelser.* Source: https://www.nrk.no/norge/nye-tall-for-ungdomskriminalitet_-okning-i-antall-ran-og-voldshendelser-1.17123685
47. Europol. 2022. *Environmental crime in the age of climate change*. Source: https://www.europol.europa.eu/publications-events/publications/environmental-crime-in-age-of-climate-change-2022-threat-assessment
48. Norwegian Broadcasting Corporation (NRK). 2024. *Saftige bøter for Svalbardturister*. Source: https://www.nrk.no/nordland/saftige-boter-for-svalbard-turister-1.16966287
49. Norwegian Broadcasting Corporation (NRK). 2024. *Filmet kongeørn med drone – fikk saftig bot på 45 000 kroner*. Source: https://www.nrk.no/vestfoldogtelemark/filmet-kongeorn-med-drone-_-fikk-saftig-bot-pa-45-000-kroner-1.16926343
50. Norwegian Broadcasting Corporation (NRK). 2024. *Rekordmange turister smugler fisk: Galskapen må ta slutt*. Source: https://www.nrk.no/tromsogfinnmark/rekordmange-fisketurister-smugler-fisk-ut-av-landet.-_-galskapen-ma-ta-slutt-sier-egon-holstad-1.16959611
51. National Criminal Investigation Service. 2025c. *Cybercrime 2024: Politiets årlige rapport om cyberrettet og cyberstøttet kriminalitet*. Source: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2025.pdf
52. National Criminal Investigation Service. 2025c.
53. National Criminal Investigation Service. 2025c.
54. OsloMet & NOVA. 2023. *NOVA Rapport nr. 11/23. Vold og overgrep mot barn og unge. Omfang og utviklingstrekk 2007-2023*. Source: https://oda.oslomet.no/oda-xmlui/handle/11250/3083676
55. National Criminal Investigation Service. 2024. *Live distant child sexual abuse*. Source: https://www.politiet.no/globalassets/tall-og-fakta/seksuelle-overgrep-mot-barn/direkteoverforte-bestillingsovergrep-dobo.pdf
56. Human trafficking coordinating unit. 2024. *Veileder: Identifisering av mulige ofre for menneskehandel.* Source: https://www.politiet.no/globalassets/rad-og-veiledning/menneskehandel/veileder-for-identifisering-av-mulige-ofre-for-menneskehandel.pdf
57. Norwegian police. 2024. *Hatkriminalitet*. Source: https://www.politiet.no/rad/hat-ytringer-og-trusler/hatkriminalitet/
58. Krasniqi, Abetare. 2024. *Hatefull motivasjon: En kvalitativ dokumentanalyse av hva domstolene vektlegger når de tar stilling til hatefull motivasjon.* Source: https://phs.brage.unit.no/phs-xmlui/handle/11250/3172963
59. Europol. 2024a.
60. Europol. 2024a.

61. Europol. 2024a.
62. Statistics Norway. 2024. *Norsk mediebarometer 2023*. Source: https://www.ssb.no/kultur-og-fritid/tids-og-mediebruk/artikler/norsk-mediebarometer-2023
63. Police trade union. 2024. *Svenske tilstander er i ferd med å bli nordiske tilstander.* Source: https://pf.no/aktuelt/medlemmer/svenske-tilstander-er-i-ferd-med-a-bli-nordiske-tilstander
64. Global Initiative Against Transnational Organized Crime. 2023. *The Global Organized Crime Index 2023.* Source: https://globalinitiative.net/analysis/ocindex-2023/
65. National Criminal Investigation Service. 2025c.
66. Økokrim. 2024b.
67. Økokrim. 2024b.
68. Økokrim. 2024a. *Nordic threat assessment on online fraud 2024*. Source: https://img8.custompublish.com/getfile.php/5349687.2528.7tsibwj7ikkslp/Nordic%2Bthreat%2Bassessment%2Bon%2Bonline%2Bfraud%2B2024-web.pdf?return=www.okokrim.no
69. Økokrim. 2023. *Nå er det NOK – Kontanter i den kriminelle økonomien.* Source: https://img8.custompublish.com/getfile.php/5229583.2528.ajuibizbuntkum/N%C3%A5%2Ber%2Bdet%2Bnok.pdf?return=www.okokrim.no
70. Økokrim. 2024a.
71. Europol. 2024b. *The recruitment of young perpetrators for criminal networks. Intelligence notification ref. No.: 2024-033*. Source: https://www.europol.europa.eu/cms/sites/default/files/documents/IN_The-recruitment-of-young-perpetrators-for-criminal-networks.pdf
72. RVTS Øst and SaLTo sekretariatet. 2024a. *Ungdom utnyttet til kriminalitet*. Source: https://www.rvtsost.no/aktuelt/ny-handbok-ungdom-utnyttet-til-kriminalitet
73. RVTS Øst and SaLTo sekretariatet. 2024a.
74. Norwegian Institute of Public Health 2020. *Barn, unge og kriminalitet: Hvordan forhindre at barn og unge kommer inn i eller fortsetter med en kriminall løpebane? Oppsummering og vurdering av virksomme tiltak, behandling or organisering.* Source: https://www.fhi.no/contentassets/9edd82a6bff54e488870e612131bb242/barn-unge-og-kriminalitet-20202.pdf
75. SVT. 2023. *Kartläggning: Unga rymmer från HVB-hem – och rekryteras av gäng*. Source: https://www.svt.se/nyheter/inrikes/kartlaggning-unga-rymmer-fran-hvb-hem-och-rekryteras-av-gang
76. RVTS Øst and SaLTo sekretariatet. 2024a.
77. RVTS Øst and SaLTo sekretariatet. 2024a.
78. Dagsavisen. 2023. *14-åring krasjet leiebil.* Source: https://www.dagsavisen.no/nyheter/2023/07/19/14-aring-krasjet-leiebil-appene-krever-ikke-bankid-hver-gang/
79. Swedish police. 2023. *Cross-agency situation report. Organised crime 2023*. Source: https://polisen.se/siteassets/dokument/organiserad_brottslighet/myndighetsgemensam-lagesbild-2023-engelsk.pdf
80. Økokrim. 2024b.
81. Ministry of Justice and Public Security. 2024a.
82. United Nations Office on Drugs and Crime. 2024. *Casinos, money laundering, underground banking, and transnational organized crime in east and southeast Asia: A hidden and accelerating threat.* Source: https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf
83. Norwegian National Security Authority. 2020a. *Temarapport – Innsiderisiko.* Source: https://nsm.no/getfile.php/133153-1591706148/NSM/Filer/Dokumenter/Rapporter/Temarapport%20innsidere.pdf
84. Norwegian National Security Authority. 2020a.
85. Dagens Næringsliv. 2024. *Etterforsker minst syv saker med utro banktjenere i Norge.* Source: https://www.dn.no/kriminalitet/okonomisk-kriminalitet/finans-norge/bank/etterforsker-minst-syv-saker-med-utro-banktjenere-i-norge/2-1-1745326
86. Europol. 2023. *The Other side of the Coin – Analysis of Financial and Economic Crime.* Source: https://www.europol.europa.eu/cms/sites/default/files/documents/The%200ther%20Side%20of%20the%20Coin%20-%20Analysis%20of%20Financial%20and%20

Economic%20Crime%20%28EN%29.pdf
87. Microsoft. 2024. *Microsoft Digital Defense Report 2024 – The foundations and new frontiers of cybersecurity.* Source: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf
88. Norwegian National Security Authority. 2024. *Risiko 2024. Nasjonal sikkerhet – et felles ansvar.* Source: https://nsm.no/getfile.php/1313477-1719434219/NSM/Filer/Dokumenter/Rapporter/Risiko%202024.pdf
89. Norwegian Financial Services Authority. 2024. *Risiko- og sårbarhetsanalyse (ROS) 2024.* Source: https://www.finanstilsynet.no/publikasjoner-og-analyser/risiko--og-sarbarhetsanalyse/2024/ros-2024/risiko--og-sarbarhetsanalyse-ros-2024/#risiko--og-saarbarhetsanalyse-ros-2024
90. NTAES. 2024. *Registermanipulasjon.* Source: https://www.ntaes.no/reports/NTAES%20Rapport%20Registermanipulasjon.pdf
91. Myhre, Thoresen og Hjemdal. 2015. *Vold, overgrep og alkoholbruk – en ond sirkel?* Source: https://www.forebygging.no/Kronikker/--2015/Vold-overgrep-og-alkoholbruk--en-ond-sirkel/
92. National Criminal Investigation Service. 2024. *Trusselaktørers kontaktetablering med barn på internett*. Source: https://www.politiet.no/globalassets/tall-og-fakta/seksuelle-overgrep-mot-barn/2024-11-27_a_trusselaktorers-kontaktetablering-med-barn-pa-internett.pdf
93. Norwegian Media Authority. 2024. *Barn og medier - Barn og unges medievaner og tilgang til teknologi.* Source: https://www.medietilsynet.no/fakta/rapporter/barn-og-medier/barn-medievaner-2024/
94. National Criminal Investigation Service. 2024. *Barn som selger egenprodusert seksualisert materiale til voksne.* Source: https://www.politiet.no/globalassets/dokumenter-strategier-og-horinger/kripos/seksuelle-overgrep/barn-som-selger-egenprodusert-seksualisert-materiale-til-voksne.pdf
95. INTERPOL. 2025. *Fisheries crime threatens food security and undermines the sustainability of our oceans.* Source: https://www.europol.europa.eu/crime-areas-and-statistics/empact
96. Europol. 2021. *EU Policy Cycle – EMPACT.* Source: https://www.europol.europa.eu/crime-areas-and-statistics/empact
97. INTERPOL. 2025. *Tackling environmental crime: Germany, INTERPOL and WWF unite efforts.* Source: https://www.interpol.int/News-and-Events/News/2025/Tackling-Environmental-Crime-Germany-INTERPOL-and-WWF-unite-efforts
98. Norges Råfisklag. 2024. *Nøkkeltall.* Source: https://www.rafisklaget.no/statistikk
99. Norwegian Veterinary Institute. 2025. *Dødelighet i lakseoppdrett litt ned i 2024*. Source: https://www.vetinst.no/nyheter/dodelighet-i-lakseoppdrett-litt-ned-i-2024
100. Norwegian Food Safety Authority. 2023. *Mattilsynets arbeid med dyrevelferda.* Source: https://www.mattilsynet.no/dyr/dyrevelferd/mattilsynet-sitt-arbeid-med-dyrevelferda
101. Norwegian Veterinary Institute. 2023. *Fiskehelserapporten*. Source: https://www.vetinst.no/rapporter-og-publikasjoner/rapporter/2024/fiskehelserapporten-2023/_/attachment/inline/1f94e174-ab61-4e71-8bf4-d58e57108321:83b28f3a356269e5a809c2729caf669e4522b560/Fiskehelserapporten%202023.pdf
102. His Majesty King Harald. 2024. *King's New Year Speech 2024*. Source: https://www.kongehuset.no/tale.html?tid=229540&sek=26947&scope=0
103. Ipsos. 2023a. *Hatytringer, trusler og desinformasjon mot folkevalgte.* Source: https://www.ks.no/globalassets/fagomrader/forskning-og-utvikling/fou-rapporter/Hatytringer-trusler-og-desinformasjon-mot-folkevalgte.pdf
104. Ipsos. 2023a.
105. Office of the Director of National Intelligence. 2024a. *Annual Threat Assessment of the US Intelligence Community.* Source: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3787-2024-annual-threat-assessment-of-the-u-s-intelligence-community
106. Office of the Director of National Intelligence. 2024. *Press release no. 29-24*. Source: https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/4015-pr-29-24
107. Office of the Director of National Intelligence. 2024a.
108. MSSP. 2024. *NATO, others targeted by novel hacktivist collective*. Source: https://www.msspalert.com/brief/nato-others-targeted-by-novel-hacktivist-collective
109. Drago. 2024. *Targeting Operational Technology: The Hacktivist's Path to Public Attention and Disruption.* Source: https://www.dragos.com/blog/hacktivist-tactics-targeting-operational-technology/
110. CISA. 2024. *Defending OT Operations Against ongoing Pro-Russia Hacktivist Activity.* Source: https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity-508c.pdf
111. The Hacker News. 2024. *Crypt Ghouls Targets Russian Firms with LockBit 3.0 and Babuk Ransomware Attacks.* Source: https://thehackernews.com/2024/10/crypt-ghouls-targets-russian-firms-with.html
112. Infosecurity Magazine. 2024. *From Protests to Profit: Why Hacktivists Are Joining the Ransomware Ranks.* Source: https://www.infosecurity-magazine.com/news-features/why-hacktivists-joining-ransomware/
113. SentinelOne. 2024. *Ikaruz Red Team | Hacktivist Group Leverages Ransomware for Attention Not Profit.* Source: https://www.sentinelone.com/blog/ikaruz-red-team-hacktivist-group-leverages-ransomware-for-attention-not-profit/

Police Threat Assessment 2025 References Menu

TIP THE POLICE OFF

By tipping the police off about offences you know have been committed or may be committed you help prevent similar incidents in the future.

→ **Tips.politiet.no**

Call the police's 24-hour line at **02800**. Is it an emergency? Call **112**.
You can also text us on **112**.

The police online patrols are visible and available on social media. They share information, receive tip-offs, reply to relevant questions and do online policing.

→ **https://www.politiet.no/rad/trygg-nettbruk/politiet-i-sosiale-medier/**

The police–business liaison officers work to prevent and reduce employer crime and crime against companies. You are welcome to contact your local business liaison officer. They are there for you and your business.

→ **https://www.politiet.no/kontakt-politiet/naringslivskontakter/**

Support centre for crime victims
Are you a victim of crime, such as violence, threats, sexual abuse or restriction of your personal freedom?

Call us on: **800 40008**

POLITIET

Police Threat Assessment 2025 - Norway

Published by: National Criminal Investigation Service

politiet.no/trusselvurdering