POLITIET

POLICE

THREAT ASSESSMENT 2026

NORWAY

PREFACE

The police's mission is to protect life, health and the shared assets and values of society. It is our job to enforce the law and maintain public safety in all parts of the country. The police must prevent, detect and investigate offences and defend due process of law. In order to succeed, we rely on public trust. The police must both tackle everyday crime against individuals and meet the largest crime threats with sufficient force.

And the organised criminals who represent the largest threats to society are becoming increasingly professionalised. Criminal networks specialise in various types of crime and purchase services from one another to shield themselves and improve operational efficiency. In their national threat assessment, the Norwegian Police Security Service explain how foreign governments engage the services of organised criminal actors, and how criminal networks can be used as proxies for state actors.

In 2025 the police uncovered a number of cases of violence-as-a-service, often referred to as VaaS. Beyond the obvious threat to public safety, it is a great concern that criminals exploit youngsters to commit violence. These developments make it harder to identify the instigators of serious crime, placing high demands on international police cooperation, police methods and prioritisations. This is significant, both for public safety and national security.

The police must adapt to a complex crime picture and a demanding geopolitical situation. If we are to succeed, we must collaborate closely with other government agencies, local authorities, businesses, civil society and international partners. With this Police Threat Assessment, we aim to share our understanding of the current situation and the challenges we are faced with in the near future. By sharing knowledge we can strengthen our joint 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 public report providing comprehensive, up-to-date insight into the crime challenges facing society. The report is an important part of the police's aspiration for transparency.

The report comprises three sections. The first section introduces the purpose and methods of the report and describes some of the key drivers expected to impact crime in the year to come. Section 2 provides an insight into the breadth of the crime picture in the past year. Section 3 describes what the police consider to be the key challenges likely to pose a threat to society this coming year.

§ THE NORWEGIAN POLICE ACT

"The State shall provide the police service needed by the community. Police duties shall be performed by the police and lensman services.

The police shall through preventive, enforcing and helping activities contribute to society's overall effort to promote and consolidate the citizens' security under the law, safety and welfare in general."

Section 1 of the Norwegian Act Relating to the Police (Police Act)

As set out in section 1 of the Norwegian Police Act, fighting and preventing crime is at the heart of the police's mission. To succeed with this mission, the police rely on the support of the general public and actors in the public and private sectors. The Police Threat Assessment may consequently also be a tool for others as part of our joint effort to prevent crime and protect the assets and values of our society.

The police work non-stop to obtain information about and gain insight into current crime trends. The report is based on information obtained from Norwegian police districts, specialist agencies and international partner organisations, including Europol, as well as various other public sources. Where sources are in the public domain, these are referenced in the report. In some cases, the only references included are statements from the police made to media outlets. Please note, however, that such statements were not the only sources used in these cases. Some of the sources are not included in the references due to confidentiality obligations.

1.2

CRIMES THAT POSE A THREAT TO SOCIETY – SOME CHARACTERISTICS

The Police Threat Assessment focuses specifically on crime that is considered a threat to society. To be included in section 3 of the report, the crimes must present a threat to society as a whole. Specifically this includes threats to *public safety, economic assets, fundamental structures of society and infrastructure and functions critical to society.*

Threats to public safety are crime threats impacting the inhabitants' movements in public places, their activities in cyberspace or their participation in public debate.

Threats to economic assets are crime threats that cause considerable damage or financial loss. This includes macroeconomic loss, for example through crime causing distortion of competition in the business sector or loss of public sector income.

Threats to fundamental structures of society are crime threats undermining the foundations of society, such as the labour market, justice system or basic democratic principles and institutions.

Threats to critical infrastructure and functions can include water and electricity supplies, banking services, health services and other vital services that society relies on from day to day.

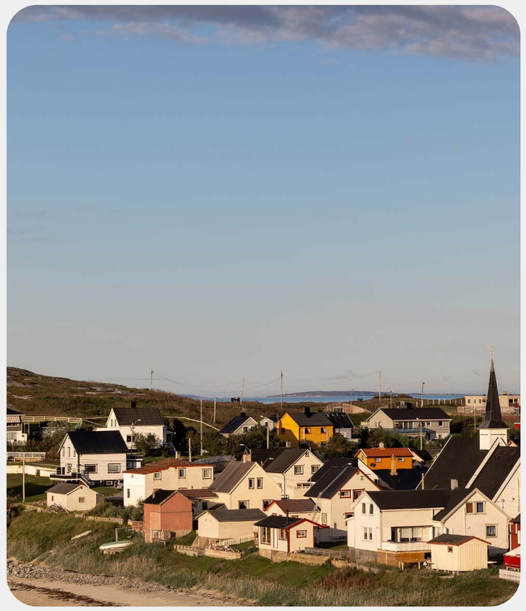


Photo: the police

1.3

DRIVERS OF CRIME

Crime arises in a complex interplay of factors that influence individuals and society. A number of drivers impact the crime picture, and most of them evolve slowly. Human factors make up the motive for or functions as a catalyst for most types of crime. Such factors are, for example, mental ill-health, boredom, willingness to take risk, desire for money, sex drive, opportunism and the desire to belong to a social group.

The crime picture has remained relatively stable over time in Norway, and changes tend to happen gradually. However, whether or not a threat has changed cannot alone be taken as an indication of its seriousness. This section of the report will focus on the drivers, some stable, others changing, behind the crime trends.

A PERIOD OF UPHEAVAL

"Ours is a time of geopolitical upheaval with fast-paced change and much insecurity. From the strengthening of democratic values and multi-lateral cooperation of the 1990s, the situation has changed fundamentally. Globalisation has ground to a halt, whilst polarisation and rivalry between super-powers are increasing. Authoritarian political movements gain momentum, including in allied countries that we identify with. The rule-based world order, which has served Norway well, is under pressure."

Statement from the Ministry of Foreign Affairs, Parliamentary White Paper no. 20 (2025)[1]

Geopolitical rivalry

Geopolitical rivalry is a key word for much of the interaction between states today. In recent years, the international system has evolved towards a so-called multipolar power structure, where countries fight for their place as global or regional superpowers. Amongst subject-matter experts, there is a wide consensus that such multipolarity tends to increase competition, mistrust and instability. This situation can impact the crime picture in Europe and Norway.

In their public threat assessments, the Norwegian Police Security Service (PSS) and the Norwegian Intelligence Service (NIS), both emphasise the threat from organised criminals acting on behalf of state actors, so-called proxy-actors.[2] According to the PSS, the lines are blurring between state actors, terrorism and organised crime. The police share their concern for a trend whereby criminal networks can be exploited by foreign governments to carry out operations.

WHAT IS A PROXY ACTOR?

Norwegian intelligence and security services define proxy actors as persons or organisations with no formal ties to intelligence and security services or other public agencies, who, knowingly or not, carry out activities on behalf or in support of state actors. The activities can be politically, ideologically or financially motivated. The Norwegian intelligence and security services have pointed out that proxy actors are put to active use in activities spanning from traditional espionage to sabotage, violent attacks and information warfare targeting the West.[3]

When crimes are committed across national borders the need for international police cooperation increases, both within Europe and with the rest of the world. Norway has signed a number of agreements on international police cooperation with other states.[4,5,6] For example, in 2025 our National Police Commissioner signed an important memorandum of understanding with Morocco setting the framework for a closer cooperation between national police forces.[7] Although fighting crime has long been a common cause for the international community, the climate for cooperation is changing due to geopolitical rivalry. Criminal actors operate from states where Norwegian police have limited possibility to prosecute them. This is particularly challenging in relation to drug crime, fraud and cyber-dependent crime. Such operational leeway for criminals can constitute a significant driver to commit crime, both in terms of scope and nature of the crimes.

Trends of the Norwegian economy, labour market and welfare schemes

According to a recent forecast report from the Ministry of Finance, prospects are good for the Norwegian economy in the coming years.[8] Despite a proportion of the population being outside the labour market, the unemployment rate is low for healthy individuals of working age. The Ministry of Finance is satisfied that, unless the global economy is hit by major unforeseen events, unemployment rates, the financial situation of families and the welfare system will remain stable. Start-up rates and bankruptcies will also remain roughly unchanged, providing a high employment rate and labour-market stability.[9] The new budget presented by the Government provides for the continuation of nearly all existing welfare and benefit schemes.

Although the general state of the Norwegian economy is good, the real estate market is still under great strain, particularly in the big cities. Almost NOK 100 billion (around EUR 9 billion) worth of real estate transactions are conducted in Norway each year without the authorities being able to track ownership in real-time.[10] The real estate market can therefore function as a driver of crime as it combines vast economic assets and complex transactions, often conducted anonymously and with a varying degree of supervision.

It is uncertain how trade wars and new customs tariffs will impact the Norwegian economy in the coming year. Norway has a special status in the European cooperation, and with a small, internationally exposed economy, the country is vulnerable to cyclical variations. The value of the Norwegian kroner has fallen in the past few years.[11] Whilst this has brought some positive consequences for the Norwegian economy, it has also reduced the buying power and increased the expenses of consumers and businesses.

What's more, the impact of inflation is both demo-graphically and geographically lopsided. Inflation has a greater impact on low-income families who spend a larger portion of their income on, for example, food and electricity. Families who are already in dire financial straits are consequently impacted more negatively by inflation than families and individuals who are better off.

The value of the Norwegian kroner has fallen in the past few years. Photo: the police

Technological developments

Technological developments are shaping almost every aspect of our lives, including the crime picture. However, it is not just technology, with its new tools and services, that evolves. Society's relationship with technology and how we use it in our everyday lives is changing.

When criminal actors adopt new technologies and change their modi operandi, known crime threats can change form and increase drastically in scope. Other crime challenges are entirely new and emerge as a result of technological developments.

"VIPPS ROBBERIES": A NEW PHENOMENON OR A CHANGE OF MO?

In 2025 robberies committed using the Norwegian mobile payment app Vipps, referred to in the media as "Vipps robberies", became the object of much attention.[12] Although sometimes presented as a new phenomenon, robberies and theft from individuals is nothing new. However, the use of digital payment solutions, with Vipps being the most widely used in Norway, has paved the way for a new method.

Electronic devices have become part and parcel of everyday life. They are an important part of how we work, obtain information and communicate with each other. Whilst the focus of the technology debate is often on children and youngsters, it is just as relevant for adults. A great many of the services we rely on in our daily lives are digital. This includes services used to communicate with government authorities, banking services, digital market places for exchange of goods and services, food delivery and transport services, and has become a fixture of the legal as well as the illegal economy. At the same time, many people lack the skills and capabilities needed to take part in an increasingly digital lifestyle and are excluded from the digital community. This can make them more vulnerable to certain types of crime committed on or with the help of digital platforms, such as fraud.

Artificial intelligence (AI) is by far the most significant and talked-about technological development in the past few years, and can become a driver of new types of crime and cause a surge in some existing crime challenges. The fast-paced development of AI and technology in general increases demand for regulatory measures to prevent crime.

The technological developments have given private companies, particularly in the technology sector, an important role in new sectors of society.[13] One example is social media, which have become an important arena for free speech, but also for crime. The extended status of tech companies gives them a key role in preventing and fighting crime.

To many, social media have become an integral part of everyday life. Whilst it is often hotly debated in relation to children and teenagers, this concerns people in all age groups. Lines between the digital and physical environment are blurring. For example, digital communication between classmates can be just as important to the school environment as what happens in the physical school yard. Experience from police cases has also shown how contact initiated on digital platforms is taken offline to physical spaces, sometimes with dire consequences. One example of this is online sexual crimes, which may ultimately open the door to hands-on sexual abuse.[14,15]

Cryptocurrencies and their associated protocols give criminals increased scope to conduct their activities. End-to-end encryption of transactions is used to anonymise senders and receivers. The legal framework is evolving, the control mechanisms of the banking sector are strengthened and obliged entities in the finance industry are becoming more vigilant. This makes it harder to include cryptocurrency as part of traditional financial services. Increased regulation has resulted in specialised actors offering money-laundering services to circumvent control mechanisms.

> *Lines between the digital and physical environment are blurring. For example, digital communication between classmates can be just as important to the school environment as what happens in the physical school yard.*

02 CRIME IN THE PAST YEAR

In addition to focusing on the crimes that are likely to pose a threat to society in the coming year, we must also develop an understanding of the breadth of crime challenges facing society. Recorded complaints alone do not paint a clear picture of the extent of crime nor of the changes in crime over time. They can, however, be included as one of many indicators in an assessment of the crime situation. The following chapter provides a brief overview of the crimes reported to the police in Norway during the past year.

Photo: the police

2.1

TYPES OF CRIME REPORTED

To what extent the number of reported crimes matches that of the actual number of incidents largely depends on the type of crime. Only for crimes that are highly likely to be detected or reported, there is a fairly good match between the number of police reports and actual incidents.

A great many incidents that are or may be interpreted as crimes, are never brought to the police's attention and, thus, not recorded as criminal cases. Reversely, no criminal offence was detected for some of the reported incidents. This can be due to both individual and societal factors. As a consequence, fluctuations in the number of criminal cases from one year to another must not be overinterpreted. Despite this, crime statistics can still provide a useful indication of what the crime picture looks like during a given period.

Violent crime

Violence or threats of violence not only harm the involved parties, they also have a detrimental effect on the perceived safety of people in the surrounding community. Violence and threats made up slightly over 10% of all crimes reported in 2025. Most reports concerned lesser violent offences (70%), whereas the most serious violent crimes[ii] constituted less than 2% of the total case volume. At a national level, the incident rate has remained relatively stable over the past ten years. Following a steep decline during lockdown in 2020–2022, incidents have returned to and stabilised at a level marginally higher than in the pre-Covid years.

The number of criminal investigations into domestic violence has risen in recent years and represents a considerable societal challenge. A proportion of the increase may be explained by a revision of police guidelines for launching investigations[18] and changed procedures in partner agencies and bodies such as child welfare services and schools.

INVESTIGATIVE CAPACITY OF THE POLICE

The investigative capacity of the police is limited, and many less serious cases fall outside the annual priorities set by the Director of Public Prosecutions.[16]

According to the 2024 annual prosecution report, very serious criminal cases[i] constituted slightly over 2% of the total caseload of the police. Despite the low number, these cases demanded more than 34% of the police's investigative resources. The least serious criminal cases, on the other hand, constituted 84% of the police's caseload in 2024, and 33% of the police's investigative resources were tied up in these cases.[17]

[i] Cases comprising homicide, sexual crimes committed against children under the age of 16, aggravated narcotic drug and doping offences, rape and domestic abuse.
[ii] Crimes such as aggravated bodily harm, attempted homicide and homicide.

Police Threat Assessment 2026 – Norway Section 02 Contents

INCREASED AWARENESS AND IMPOSITION OF VISIT AND CONTACT BANS

Visit and contact bans is one of the tools the police have at their disposal to prevent violence and threats. This implies that a person is banned from being in the vicinity of a given person, pursuing, visiting or in any other way contacting them. Under certain circumstances such bans may also include electronic monitoring, known as "GPS tagging".[19] This makes the police better able to respond quickly and avert potential threats and violent crimes.

Over the past few years, the police have imposed an increasing number of such bans, including in combination with GPS tagging.[20,21]

The number of homicides recorded in Norway in 2025 was unusually low.[22] 19 people were murdered, the lowest number on record since 1990. It is, however, important not to attach too much weight to this, as the dataset is small, and any changes cannot be interpreted in isolation but should be seen in the context of a period spanning several years. The number of homicides has been stable since 1990, with an average of 28 cases per year.

In homicides, there is a clear over-representation of male offenders (78%) and an over-representation of female victims (58%). Establishing the motives for murder can be difficult, but hardly any of the cases are linked to conflicts between criminal networks. Almost all of the victims knew or were acquainted with their murderer, and in around half of the cases, the victim and offender were close.[23]

The number of attempted homicides recorded (52) was also somewhat lower than in the two previous years.[iii] The average age of the perpetrator was lower in cases concerning attempted homicide than in cases of homicide. Here, men were hugely overrepresented amongst perpetrators (87%) as well as victims (73%). Conflicts between criminal networks are more frequently cited as a motive for attempted homicide than for homicide.[24]

> *All victims knew or were acquainted with the perpetrator, and in around half of the homicides, the victim and offender were close.*

[iii] 2024 (58) and 2023 (61).

Sexual offences

The number of sexual offences reported to the police has fallen slightly in the past two years. Around 2% of all reported offences in 2025 were sexual offences. Around a third of the complaints for sexual offences concerned rape.

Sexual offences against children constitute almost half of the reported sexual offences, with the largest sub-category by far being sexualised imagery of children. This sub-category makes up in excess of 40% of the complaints of sexual offences against children. The circumstances in which an offender may come into possession of or share sexualised imagery of children are legion. Although many cases involve adult offenders, there are also examples of children and teenagers being reported to the police for being in possession of or sharing sexualised images or videos of other minors.

In recent years, there has also been an increase in cases involving sexual extortion, so-called sextortion. A common characteristic of these cases is that the victims face threats of publication of sexualised imagery.[26] This may be imagery originally shared by the victims themselves, imagery which has come into the wrong hands or AI-generated imagery. The National Criminal Investigation Service has previously described how some children and teenagers generate sexualised material that they offer for sale to adults. In some cases, this may lead to hands-on sexual abuse.[27]

Acquisitive crime

There are many incentives for victims to report acquisitive crimes, for example to be able make a claim on their insurance. Acquisitive crime amounts to as much as 35% of all criminal complaints. The victims can be private individuals or businesses, such as shops. The total financial loss from acquisitive crime is not known, but it is estimated at billions of Norwegian kroner.

The number of police reports of acquisitive crime has been relatively stable in the past years. The police recorded an increase in reports of shoplifting in 2025, but this may be due to the introduction of digital solutions for the reception and processing of complaints. These solutions have made it easier for businesses to report shoplifting offences and reduced processing time for complaints.

NEW LEGAL PROVISION ON SEXUAL CONSENT: ONLY "YES" MEANS "YES"

The new legal provision on sexual consent, sometimes referred to as the "consent law", came into force on 1 July 2025. The new provision introduces the requirement for active consent.[25]

Section 291 of the Norwegian Penal Code now reads as follows:
"A penalty of imprisonment for a term not exceeding 6 years shall be applied to any person who engages in sexual activity with a person who, neither in words nor in actions, has consented thereto."

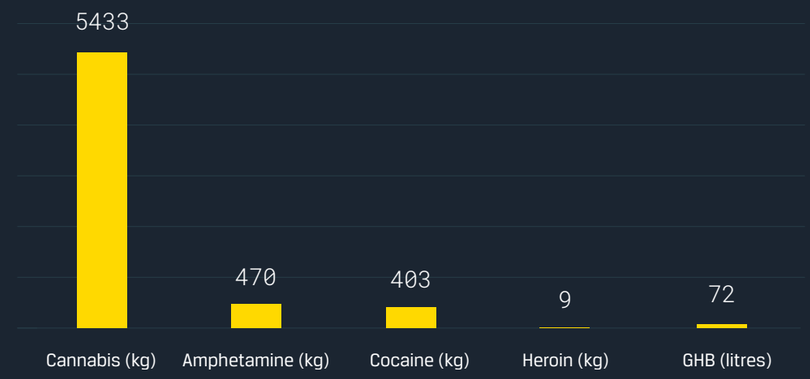
It is too soon to say whether this amendment will have an impact on the number of reports and convictions of rape. This is part of a wider trend whereby a number of other countries have adopted similar legislative amendments.

GRADUAL ROLL-OUT OF AN ONLINE SOLUTION FOR CRIMINAL COMPLAINTS

The police's adoption of new digital solutions has lowered the bar for private individuals and businesses to report crimes. The police's online solution for criminal complaints has been rolled out gradually since 2019. In its early stages, the solution was only available to private individuals, but from 2025 businesses have also been able to report certain types of offences, such as shop-lifting, online. Certain parts of the processing of criminal complaints have also been automated.

This implies a slight change in how cases are recorded, and crime report figures may be impacted during a transition period. Added to this is a possible increase in complaints due to the ease of use of the new solution. However, it must be noted that the solution only includes certain offences, and that many criminal complaints must still be made in person to the police.

The police keep statistics of narcotic drugs seizures, including seizures by the Customs service. In 2025, there were 16,632 such cases. Excessively large quantities of hashish and marijuana were seized in 2025. Only once before, in 1995, has more cannabis been seized in a single year. Cocaine was up from 2024, both in terms of the number of seizures and volume. The number of heroin seizures also increased slightly although the seized quantity was at its lowest since 2007, and the average potency of the drug is at a historic low.[29]



Drug crime

Violations of narcotic drugs and doping legislation make up around 5% of the total number of criminal cases. These offences are detected and prosecuted almost entirely based on the efforts of the police, customs service, postal services and other authorities.

The number of criminal cases was down by 8% from 2024 to 2025, but was almost the same as in 2023. However, when considered in a ten-year-perspective, the number of criminal cases concerning drug crime has fallen sharply, reaching a low in 2022. The fall can almost exclusively be explained by the reduction in cases concerning drugs for personal use, as opposed to more serious drug trafficking or distribution cases. This should be seen in the context of the shift in the police's attention over time towards distributors of drugs rather than individual users.[28] The number of cases concerning use of illegal doping substances fell by 15% from 2024 to 2025.

Photo: the police

Photo: the police

Economic crime

Despite its covert nature, economic crime impacts large numbers of people by draining the government, businesses and private individuals of vast financial resources. In a survey, nearly 20% of local authorities and 7% of other businesses and organisations, claimed to have suffered losses as a consequence of financial crime.[30] In 2024, the direct loss was estimated at between NOK 43 and 64 billion (EUR 3.8–5.7 bn).[31] These are funds that could have been spent to finance education, public transport, elderly care and other political priorities. Criminal cases categorised as economic crime made up 10% of reported crimes in 2025.

As much as 85% of reported economic crime is fraud, i.e. matters where someone, through manipulation or lies, deceives others into transferring assets to themselves. Assets defrauded from individual citizens span from a few hundred Norwegian kroner (for example where the fraudster receives payment through a digital market place but fails to ship the goods to the buyer as agreed) to several hundred thousands (for example in the case of travelling builders defrauding vulnerable elderly people of their money). Fraud against private individuals is a particular challenge as the victims are often amongst society's most vulnerable, and the losses tend not to be covered by insurance.

Fraud against businesses can in some cases amount to several hundred million Norwegian kroner (tens of millions of euros). According to an estimate by the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim), Norwegian private individuals and businesses were defrauded of NOK 2.1 billion (around EUR 190 million) in 2024.[32]

Tax fraud and false accounting still make up an important category, and since 2024, there has been a marked rise in the number of such criminal cases. Corruption remains a limited phenomenon in Norway compared to other countries[33] with only a few dozen criminal cases opened in 2025. Cases categorised under the umbrella of identity theft and identity fraud constitute a bigger challenge in terms of volume as this is a key component in many types of crime. Nevertheless, in 2025 this category of crime fell by around a third on the previous year.

Cyber-dependent crime

In a global perspective, there has been a clear increase in all types of crimes targeting computer systems over the past few years. The main causes is the increased availability of artificial intelligence (AI) as a supporting tool and the commercialisation of cybercrime services.[34]

At the same time, results from a survey carried out by the Norwegian Business and Industry Security Council in 2024[35] showed that as little as 24% of organisations victims of data intrusions or data theft had reported the offences to the police. The police are well-aware that denial-of-service (DoS) attacks and computer intrusions are rarely reported to the police. Incident management is often outsourced to private actors whose focus is to contain damage in the organisation targeted by the attackers.

Ransomware attacks and other forms of extortion in the wake of computer intrusions constitutes a high proportion of the cases. In 2025, at least 17 different ransomware applications were used in cyber-attacks against small and medium-sized businesses in Norway. The police are not aware of any large enterprises being targeted in the same period.[37]

In 2025, the police recorded 349 criminal cases of computer intrusion. In many of them, the victims were private individuals. The number of such cases recorded in 2025 had trebled compared to 2023.

CYBERCRIME

Although the term covers an array of crimes ranging from minor to serious, cybercrime can be defined as illegal activities in which advanced technology either constitutes a target in itself or is utilised to facilitate crime. The distinction is often made between cyber-dependent and cyber-enabled crime.

An example of cyber-dependent crime is the intrusion into a company's computer systems. Cyber-enabled crime, on the other hand, can for example be the use of common encrypted messaging services and forums or artificial intelligence to manipulate potential victims of fraud or sexual abuse.

DENIAL-OF-SERVICE ATTACKS

The purpose of a *denial-of-service attack*[iv] is to deny, disrupt or disturb access to a server, service or network. This can for example be done by deliberately overloading the target's data traffic capacity.[36]

[iv] Shortened to *DoS*.

Photo: the police

Human trafficking

Human trafficking is when someone uses violence or threats, exploits a vulnerable situation or uses other kinds of improper behaviour to force, exploit or deceive another person into, for example, prostitution, forced labour or forced services, or into committing crime. Although the number of criminal complaints filed for human trafficking in Norway remains low, the number of unreported cases is assumed to be high.

In a global perspective, the UN considers human trafficking as one of the world's biggest criminal industries alongside drugs and arms trafficking.[38,39,40] Through international conventions, Norway is committed to preventing human trafficking, prosecuting perpetrators and identifying and protecting presumed victims.[v,41]

People who have been trafficked, rarely identify as victims. They are therefore unlikely to contact the authorities or seek help from organisations. Emotional, financial and social dependence on networks or family are vulnerabilities that can be exploited. Such factors contribute to keeping the reporting rate low compared to other crimes.

Foreign nationals are especially vulnerable to exploitation. Construction, transport, hospitality and catering, vehicle repairs, car valeting, cleaning services and agriculture are some of the industries that are overrepresented in cases involving forced labour. Victims linked to prostitution tend to be women from other countries who are staying in Norway for short periods of time.[43] Recently the question has also been raised whether cases involving minors who have been recruited to commit violence, should be prosecuted as human trafficking.

A NEW NATIONAL STRATEGY AGAINST HUMAN TRAFFICKING

In June 2025, with a view to bolster the country's efforts to fight human trafficking, the Norwegian Government presented a national strategy against human trafficking for the years 2025–2030.[42] The strategy comprises four key areas, namely coherent and coordinated efforts; prevention; assistance and protection; and prosecution. The strategy's chapter on prosecution prescribes extensive measures to strengthen the police's proactive efforts against human trafficking. To expose human trafficking, it is crucial that police and other authorities have the knowledge required to recognise the signs that someone is being trafficked.

[v] These include e.g. the Palermo Protocol and the Council of Europe Convention on Action against Trafficking in Human Beings.

2.2

GEOGRAPHICAL VARIATIONS

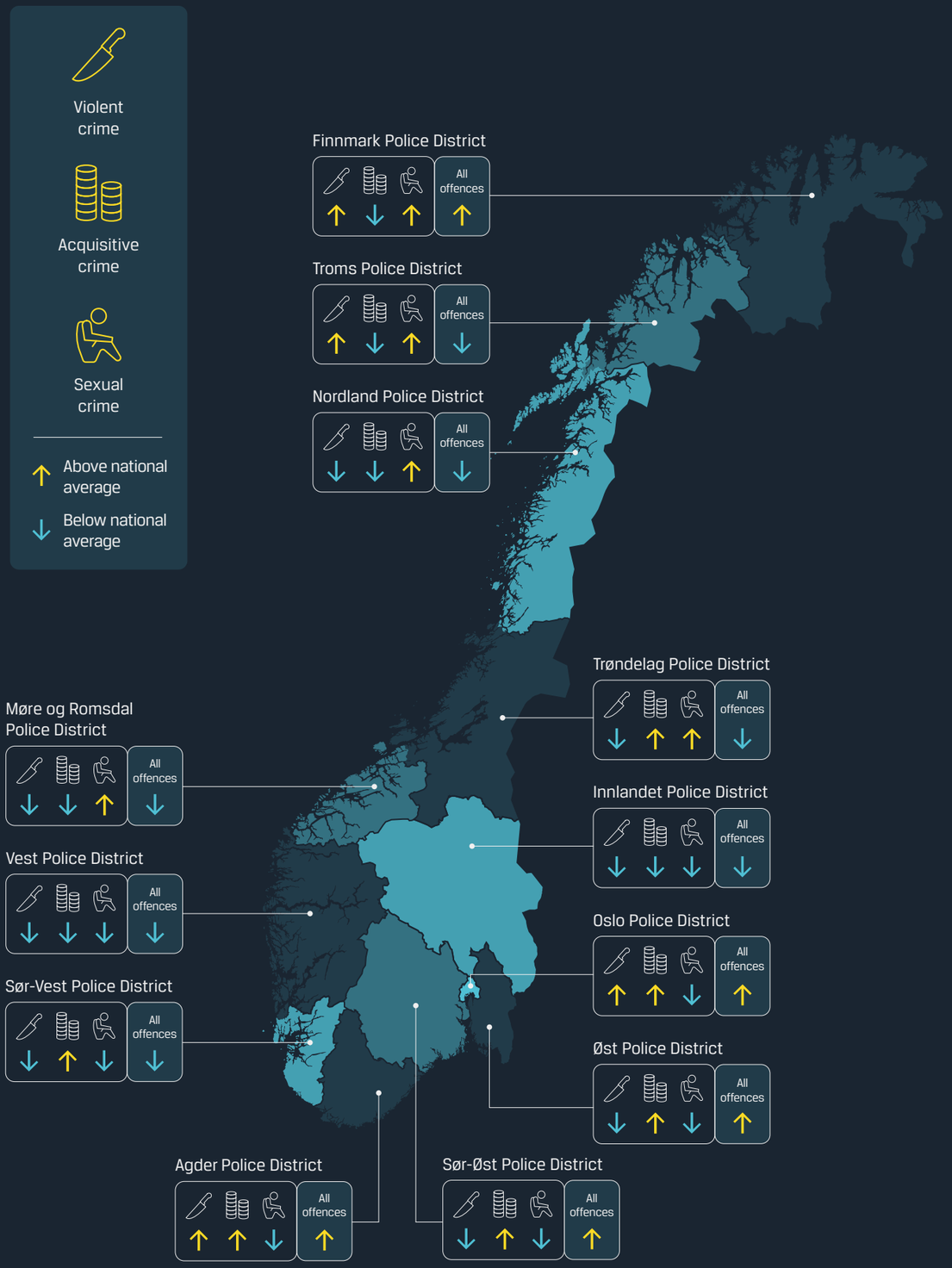
Few European countries are more geographically diverse than Norway. Its inhabitants live in areas spanning from the continuous urban belt of the south-east, via the sparsely populated inland areas in central Norway to small rural municipalities along the coast, where life in the local community typically revolves around a handful of cornerstone businesses.

The diverse climate also shapes how crime is committed. The contrast is striking from the relatively mild climate of the south to the Arctic cold and changing daylight conditions of the North. Demographics are varied too: Most cities have a young population with a sizeable migrant contingent, whereas the rural population is older, more homogeneous and male-dominated.

This creates different contexts in which crime is committed. The profile of perpetrators and victims differ widely depending on were the crimes are committed. Specific features of an area may impact the type and frequency of crime. For example, in city centres and areas around public transport hubs there tends to be a higher occurrence of crime likely to negatively impact perceived public safety.

Photo: Shutterstock

> *It's because that's where the people are. It's easy to get to. Regardless of where they are in the municipality, everyone can get to the city centre.*
>
> **Experienced police officer**



Police Threat Assessment 2026 – Norway Section 02 Contents

Oslo Police District is the district with the highest number of criminal cases in the country. This is hardly surprising as the police district covers the country's capital, which is also its biggest city.[vi] Although it is the smallest in terms of area, it is the Norwegian police district with the highest number of inhabitants. Also setting Oslo PD apart is the number of criminal cases per 1000 inhabitants, which is far higher than in all other police districts. Another interesting detail is that a lot of people who do not live there, stay in or travel through Oslo every day.

As many as half of the country's reported crimes are committed in Oslo, Øst and Sør-Øst, which are the three police districts with the highest number of reported crimes. 44% of the country's inhabitants live in the area covered by these three police districts. The considerable overlap between some of the crime challenges and the criminal networks based in the central south-eastern part of Norway means that the three districts should be treated as a whole.

Agder and Finnmark are two other police districts with a high number of reported crimes per 1000 inhabitants. At the other end of the scale are Møre og Romsdal, Vest, Innlandet and Nordland police districts. Finnmark has the lowest number of inhabitants but is the second largest district in terms of geographical area. However, as it is the police district with fewest reported crimes in absolute figures, a small variation in the number of criminal cases will produce a dramatic shift in the crime rate per 1000 inhabitants.

Much of the serious crime takes place in the big cities. Even when adjusted for population size, reports of violent crime in Oslo police district are far above the national average. This becomes especially evident in some of the most serious, non-domestic cases of violence such as aggravated bodily harm, attempted homicide and homicide. In greater-Oslo, the violent crime trend is stable. Other police districts with a high incidence of violent crime in relation to population size are Agder, Troms and Finnmark.

Although physical acquisitive crime is largely an urban phenomenon with a higher incidence in the bigger cities of the South-East, Agder and Trøndelag also have a high number of cases. If we only look at aggravated acquisitive crime, the picture is somewhat evened out, but the big cities remain over-represented. Northern Norway and the rural coastline has a low overall rate of this type of crime, regardless of seriousness. For fraud, which is often digital, the regional differences are much less marked. Even so, the central South-East is somewhat over-represented in the statistics.

Although sexual abuse happens in all parts of the country, the trend has been clear over a number of years: the northernmost half of the country is over-represented in terms of reported sexual offences per 1000 inhabitants. Some other sparsely populated districts are also over-represented in the statistics, whereas the central South-East is below the national average. This trend is opposite to that of many other types of crime.

[vi] Oslo PD includes the municipalities of Asker and Bærum.

03

CRIME LIKELY TO POSE A THREAT TO SOCIETY IN THE YEAR TO COME

This chapter presents a selection of threats that the police must target specifically in the future. It focuses on the drivers of crime and the evolution of crime in the past year. The crime is referred to as a threat to society as it has a potential to harm or weaken shared assets and values of our society (see chapter 1.2).

Photo: the police

3.1

A SIGNIFICANT, PERSISTENT THREAT FROM CRIMINAL NETWORKS

Norwegian society faces a considerable, persistent threat from criminal networks. The networks are adaptable, and continue to cooperate dynamically across national borders and continents. The fight against these networks is demanding in terms of time and resources, for the police as well as for their partner agencies and organisations.

According to Europol, organised crime is one of the greatest security threats facing Europe today. It is evolving at an unprecedented pace, changing rapidly and adapting to a world in flux.[44] This crime undermines fundamental societal structures and economic assets through violence, corruption and handling of proceeds of crime. In the past year, criminal networks have increasingly recruited and exploited minors to commit serious violence-as-a-service (VaaS) in Norway. This affects the overall safety and security of the population in public and digital spaces.

Recruitment to VaaS assignments on digital platforms is only one of the ways criminal networks utilise technology to facilitate crime. The networks often use technology that has been developed for legal commercial purposes. Encrypted messing services and eSIM cards are used to conceal communication, social media are still used as market places for drugs, and cryptocurrency is utilised as a money-laundering tool.

Photo: Shutterstock

Criminal drug networks are particularly prominent

All police districts have criminal networks who operate locally or in a handful of police districts. Many of them have their main operations in Norway but partner up with actors in other countries. The criminal networks are motivated by profits and exploit vulnerabilities in legislation and control mechanisms implemented by authorities or private organisations. Conflict levels are lower in Norway than in some of our neighbouring countries. Despite this, there are latent conflicts between some of the networks.

Some types of crime offer profit opportunities setting them apart from others. This is particularly true for drug crime, where the high demand for narcotic drugs constitutes an important driver.[45] Another frequent feature of drug crime is the use of violence in public places.[46] Many of the actors with ties to drugs networks have been involved in serious violent incidents, and some have access to firearms. Over the past year, there have also been a number of drug-related violent incidents in Norway initiated by international criminal networks.

Drug-trafficking is the primary activity of many of the most prominent criminal networks in Norway. This comprises illegal importation, distribution and sale. The networks also commit other types of crime, such as fraud, money laundering and violent crime to facilitate drug trafficking.

The degree of organisation and complexity of the networks varies greatly, but a common denominator is a clear-cut hierarchical structure and loose collaborations between actors. Some networks consist of a central core of actors and a peripheral circle of more loosely associated actors. Many networks show great resilience in that they manage to keep the drug-trafficking activities going despite the arrest of key actors. Either the jailed actors are replaced by others, or they continue their criminal activities from prison, for example using a mobile phone.

Many drug sales networks in Norway are local outfits. Their activities are primarily carried out within a limited geographical area. There is increased concern that networks actively recruit minors into criminal activities. The networks attract minors by showcasing a lifestyle of status, loyalty, firearms and money. Many of those who hold leading positions in the criminal networks today, started their criminal career as errand boys for established criminal actors.

Several key drug-trafficking networks are run by kingpins in other countries. These kingpins often hold dual citizenships, making it possible for them to stay abroad. Some have had dual citizenship from birth, others have obtained a second citizenship later in life, for example through citizenship-by-investment programmes (CBI). CBI programmes are schemes whereby certain countries grant citizenship to foreign investors. Dual citizenship complicates the extradition of criminals to Norway. This, in turn, provides increased operational leeway for criminal actors, and the police must cooperate with foreign authorities to have them prosecuted abroad.

CRIMINAL CULTURES

Certain substrata of society are marked by a criminal culture in which internal codes and values weigh heavily. Actions showing loyalty, strength and bravery tend to be brought to the fore. Some young people seeking a sense of belonging, safety and mastery are drawn to this. Certain criminal actors also exploit the lifestyle of criminal sub-cultures to control and recruit young people.

Youngsters can join a criminal sub-culture in an attempt to find an alternative path to success, status, resources and protection. The behaviour, knowledge and skills obtained through criminal cultures are seldom transferable to other areas of society. This can in turn make it difficult to break away from criminal activities and circles.

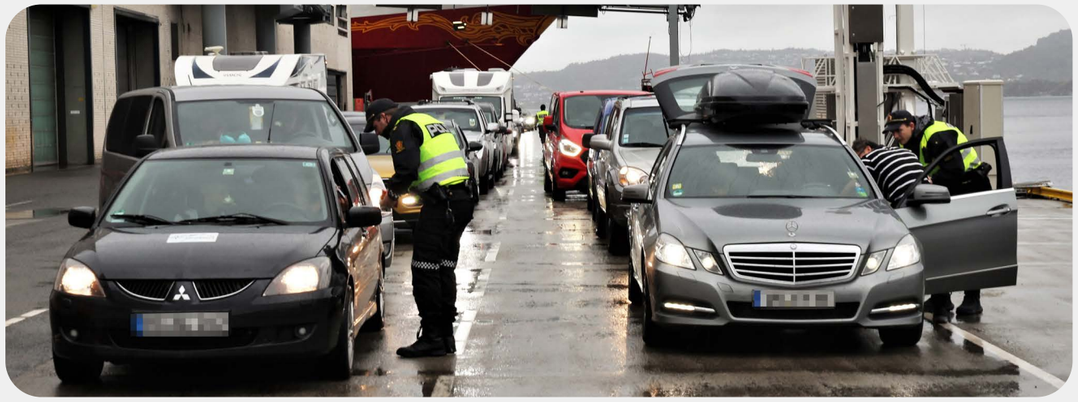


Photo: the police

Some drug networks operate opportunistically in project-based structures to procure drugs. Certain sales networks have regular networks and actors who secure the supply of drugs. Others purchase parts of larger consignments from other actors who have smuggled them into Norway. This makes drugs readily available to networks with sufficient financial means. Further, it contributes to keeping the illegal drugs market going in the event that key actors are arrested.

Other actors and networks step up whenever there is a gap in the supply chain, and the networks cooperate to continue operations regardless of conflicts and loyalties. The networks cooperate opportunistically in sales operations with actors in other parts of the country. Support services such as laundering proceeds of crime, collection and transport of drugs are often purchased from other criminal actors offering such services.

The drug market decides the scale of activity of criminal networks

Surveys based on self-reporting show that the proportion of the population who use illegal substances, both teenagers and adults, has risen sharply in recent years.[47] The total number of users is high, and a significant proportion of them are young. The size of the criminal networks is largely determined by the supply and demand generated by these consumers.

Digital platforms and social media make it easy to buy drugs for personal use without having to know or seek out the dealer in person. Criminal networks and actors use emojis and nicknames as codes for the drugs on offer.

There are big geographical variations, and urban areas have a higher proportion of users than rural areas. Overall, the proportion of users of illegal substances is higher in the greater Oslo area than in the rest of the country.[48] Over the past few years, there has been a particular increase in the use of cocaine and cannabis, and Norwegian police have also noted an increase in ketamine use, like in many other European countries. Whilst only a small proportion of users drop out from education or employment, a considerable number will develop dependency or mental health issues, fall victim to crime or experience difficulty with interpersonal relations.[49] Although the fall in fatal overdoses has been significant over time, drug use is still fatal to some.[50]

CRIME-AS-A-SERVICE

The term *crime-as-a-service*[vii] describes how illegal services are being bought and sold. The services offered span from computer intrusion to money laundering and violence, just to mention a few. When violence is sold and bought by criminals, this is referred to as *violence-as-a-service*[viii].

[vii] Shortened to *CaaS*.
[viii] Shortened to *VaaS*.

Police regularly monitor the price level of various types of drugs at different levels of the supply chain. This has shown that drug retail prices have remained relatively stable in the last decade. Prices paid by sales networks to secure drug consignments from distribution and import networks have, however, fluctuated more. A comparison of these prices shows that the sales networks' profit margins are extremely high. The illustration shows the profit margins for some common recreational drugs.

There are also regional differences, and drug prices tend to be somewhat higher in other parts of the country than in Oslo.

This is probably due to the better functioning market in the central parts of south-eastern Norway: the sheer size of the market means that there are more competitors and possible synergies within a restricted geographical area. The fact that drug prices in Norway are amongst the highest in Europe, contributes to make the market attractive to transnational criminal networks.

Norwegian and foreign authorities seize large quantities of drugs at different stages of the production and distribution chain. Although the seizures appear large, this is only a fraction of the drugs intended for the Norwegian market. An extensive research project commissioned by the EU Commission has shown that the efforts by European police against criminal networks involved in the distribution of cocaine have not had the desired effect, neither on retail prices nor on availability.[52]

PROFIT MARGINS

Cannabis	x2 .5
Cocaine	x2
Amphetamine	x6
Heroin	x8
MDMA	x11

The illustration shows the profit margins achieved by supply networks for various types of drugs in 2025.

DRUG-INDUCED DEATHS

In 2024, 342 drug-induced deaths were recorded in Norway, relatively evenly spread across the country. Accidental poisoning was recorded as cause of death in the vast majority of these cases. A clear majority of drug-induced deaths were linked to opioids. By contrast to previous years, heroin was not in the top three of the drugs causing the deaths.[51]

Norway as a destination and transit country for cocaine

Cocaine is produced in South America and mainly smuggled to Europe by sea, either directly or via ports of transit. Several major European ports have tightened control measures. Meanwhile, demand for cocaine is high. This means that an increasing number of ports is used for smuggling.[53] Moreover, Norwegian ports could increasingly be used as ports of transit for cocaine destined for the European market.

Europol expects violent crime committed by criminal networks to spread to more countries and regions as an increasing number of ports are used for cocaine smuggling. In Europe such violence has been widespread in the vicinity of some major smuggling ports and other areas central to the drug trade.[54]

Minors exploited by criminals to carry out VaaS

2025 saw an increase in the recruitment and exploitation of minors to carry out violence-as-a-service in Norway. The upward trend started in spring but rose sharply in autumn with incidents which included the use of hand grenades and firearms in public places.

Violence-as-a-service means that criminal actors and networks both supply and commission violent services, which are offered against payment. Many perpetrators are minors. The exploitation of minors evidence a high degree of cynicism in criminal networks. VaaS assignments are offered through digital platforms functioning as market-places for the commission, coordination and facilitation of violence. As well as commercialising violence and making it more accessible, this has helped secure a high degree of anonymity.[55]

The use of social media and encrypted messaging services is key to facilitate VaaS. What's more, their use bring instigators and perpetrators of VaaS together across vast geographical distances.[56] The instigators are part of established criminal networks and protected by stringent security measures. Some operate from abroad, particularly from countries without an extradition treaty with Norway.

In many cases, perpetrators do not learn the motive behind the assignment or the identity of the victim until they have accepted it. VaaS assignments have increasingly been advertised, planned and carried out within a short space of time, sometimes as little as hours or days. This makes VaaS an international problem which is difficult to prevent and combat.

The police averted dozens of VaaS assignments in 2025. The averted assignments involved minors from all parts of the country.[57] Some were below, others above the age of criminal liability. Some were known to the police, others were not. Norwegian minors have also been recruited to carry out VaaS in other countries. Young perpetrators are lured with promises of money and status, but the promises are rarely kept. In many cases the young perpetrators are not paid, and many have been arrested following the assignments.

Young perpetrators in the VaaS chain (see illustration) are often asked to send photos of their identity documents, such as passports, and confirm their identity in video calls. The police have seen that some potential perpetrators who have withdrawn from the assignment mid-process, have become victims of threats. The criminal networks exploit the youngsters' forwarded personal details. This method is also known from Sweden. The police are concerned that young people who are recruited to commit VaaS may become victims of pressure, coercion and threats from criminal networks both prior to, during and after the assignments.[58]

VaaS committed in Norway is generally linked to Swedish criminal networks. In the past, criminal networks relied on resources from Sweden. Now, the perpetrators are often locally sourced minors.[59] Swedish criminal actors have used VaaS to strengthen their own position and capacity for violence in the Norwegian drug market, which to them is an attractive market.

VaaS is mainly used against other criminal actors. However, with minors armed with weapons such as hand grenades committing the attacks, the risk of confusing targets or harming innocent persons is high.

Police Threat Assessment 2026 – Norway Section 03 Contents

Recruitment of youngsters to carry out violent offences

Youngsters can be recruited into VaaS in a number of different ways, but the process tends to follow a pattern involving a fixed set of roles.

INSTIGATOR

The person who orders and finances the crime. Often based abroad and part of an established criminal network.

RECRUITER

Functions as an intermediary. Places VaaS "job ads" in online groups or other channels to recruit perpetrators.

ENABLER

Someone who enables the crime by procuring weapons, facilitating transport and finding places to stay. More than one enabler can be involved in the same crime.

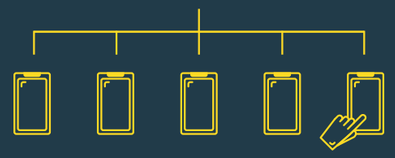
PERPETRATOR

The person who physically commits the commissioned violence. Generally youngsters with no links to the criminal network who neither know the victim nor the area where the crime is to be committed.

Minors are recruited into VaaS on digital platforms

Criminal networks publish content targeting youngsters on social media such as Instagram, TikTok and Snapchat. Here, the networks place ads and recruit young people to commit VaaS. Algorithms help spread the content far and wide. The recruiters use memes and gaming terminology to downplay serious violence.

STEP 1



Recruiters get minors to join them on more secure apps where they can communicate in closed groups. In the groups, recruiters publish generic descriptions of the VaaS to be carried out. The same jobs are published on several forums to be sure to find potential candidates.

STEP 2

For the planning and coordination phase, security is tightened further and communication is moved to end-to-end encrypted apps such as Signal. The details of the VaaS to be carried out can now be shared directly with the perpetrator.

STEP 3

3.2

CRIMINALS MAKE A PROFIT FROM SOCIETY'S SHARED ASSETS AND VALUES

The criminal economy in Norway has previously been estimated at around three per cent of the country's mainland GDP.[60] Illegal economic activity causes a massive loss of tax revenue for the public sector. To the extent that organised criminals succeed with their crimes at the expense of society, this can, in the longer run, erode trust in the system and undermine the welfare state.

The lines between traditional economic crime and other profit-motivated crime continue to blur as organised criminals are increasingly involved in economic crime. There is a lot of money to be made on fraud against actors in the public and private sectors. The public sector strives to become more user-friendly and transparent with new digital solutions at the public's disposal. This increases availability but can also facilitate crime.

Proceeds of crime are increasingly handled by professionals. Actors specialising in money laundering have developed a range of unregulated financial services outside the traditional finance sector, paving the way for a parallel financial underworld for criminal actors. The proceeds remain in the hands of the criminals and are reinvested in the criminal economy.

THE CRIMINAL ECONOMY

The criminal economy is the complete system of activities, transactions and services where economic assets are generated, transferred or concealed through actions that, in whole or in part, are carried out outside of legal and regulated structures and processes.

Based on this definition, Swedish authorities have estimated the Swedish criminal economy at 352 billion kroner per year, or 5.5% of the country's GDP in 2024.[61]

Photo: the police

> *In 2025 frauds estimated at over NOK 2 billion (around EUR 180 million) were reported to Norwegian police.*

Digital IDs misused to commit fraud

Every year public organisations, private businesses and private individuals fall victim to different kinds of fraud. In 2025 frauds estimated at over NOK 2 billion (around EUR 180 million) were reported to Norwegian police. By way of comparison, the estimated loss from fraud in the Nordic countries in 2023 was estimated at EUR 828 million or around NOK 10 billion.[62] The actual loss is probably much higher.[63] Profits from fraud can help finance new fraud schemes, but also enable other criminal activities.[64]

DIGITAL ID FRAUD

Criminal actors use digital data such as personal details, passwords and bank details to commit fraud. This can for example be done by gaining control of digital identities. The most widely used digital ID system in Norway is BankID.[65]

Criminals can gain control over other people's digital IDs, for example through purchase, theft, extortion or threats as a means to make victims carry out certain actions using their own digital ID.[66] Foreign employees who are victims of work-related crime in Norway also risk becoming victims of digital ID fraud.[67] Another method involves the use of artificial intelligence.[68] International actors have developed applications that pose as well-known and trusted Norwegian institutions to gather card details from private individuals. This way, they have obtained the card details of thousands of Norwegian citizens.[69]

Identity fraud is an ingredient of many different types of fraud. One example is online banking fraud, where fraudsters misuse digital personal details to access bank accounts, which can then be emptied of significant amounts of money. Another widespread phenomenon is loan fraud. One such scheme consists in taking out car financing or a home loan from a finance institution by misusing someone else's identity. Another one consists in the misuse of digital IDs for credit assessments in connection with loan applications. In some cases, there is a suspicion that insiders in banks or credit agencies have ensured that the loan applications were granted.[70]

Through digital ID fraud and manipulation of public records, the public purse can potentially be drained of millions. Identity fraud is one of the methods used by criminals to exploit the system and receive undue benefits from the Norwegian Labour and Welfare Administration or the Tax Administration.[71]

Welfare fraud and misuse of public funds threatens the Norwegian welfare model

Welfare fraud and misuse of public funding pose a significant threat to the Norwegian economy and welfare model. Criminals are regularly found to be exploiting public schemes intended to, inter alia, secure the financial basis of the welfare state or fund various welfare schemes or environmental protection measures. The methods include the use of false documents, identity fraud and manipulation of digital application processes or public records. The risk of fraud is particularly high in trust-based schemes with a low degree of supervision. Whilst more new digital systems and administration processes may increase efficiency and user-friendliness, they may also facilitate crime.[72] The consequences are far-reaching: the public sector loses money, trust in public benefit schemes is eroded and more funds are channelled into new crime.

The public welfare model is largely financed through the taxation of income, consumption and wealth. Evasion of VAT and other taxes are examples of economic crime causing a great loss of income to the government. In many cases, forged documentation has been used to justify VAT refund claims for businesses that are not actually trading. Digitalisation and new technology means that this type of crime is committed at a faster pace and on a larger scale than before.[73]

The police have not been able to quantify the extent of benefit fraud. However, estimates from the Norwegian Labour and Welfare Administration (NAV) in 2024, including both fraud and non-fraud overpayments, indicate that it could amount to around NOK 5 billion (around EUR 450 million) a year.[74,75] In some of the more complex frauds committed against NAV, individuals have created fake jobs or inflated the number of hours to be able to claim various welfare payments. This often demands meticulous planning and close collaboration between the person receiving the payments and the employer. The actor set-up is complex and in some cases includes links to criminal networks. Misuse of public benefit schemes is a secondary activity of these networks.[76]

Environmental subsidy schemes are also exploited. Not only does this harm the economy but also the environment by undermining public environmental protection measures. The total payments from these schemes amount to several billion Norwegian kroner. Over the last few years, a number of persons have been convicted of fraud in connection with such subsidy schemes.

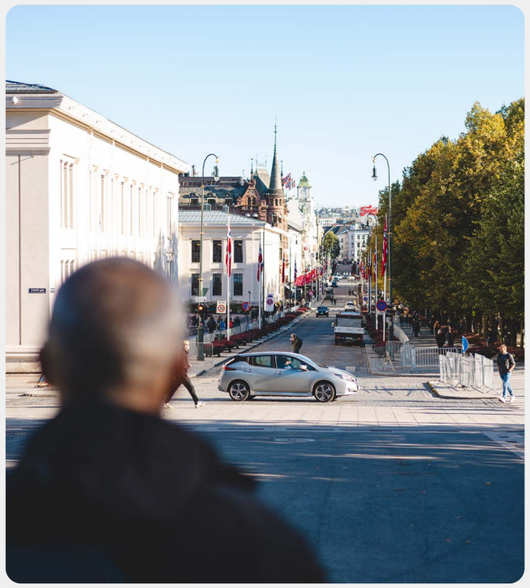


Photo: Shutterstock

MISUSE OF TAX REFUND SCHEME FOR FLUORINATED GASES

Fluorinated gases (F-gases) are used as coolants in cooling systems, air conditioning systems and heat pumps, amongst other things. Such gases are extremely harmful greenhouse gases and consequently subject to heavy import taxes. To ensure the safe treatment of used gas, a scheme has been introduced whereby the import tax is refunded upon return to the authorities of the used gas bottles.

In 2023 a man was found guilty of serious fraud having defrauded the Norwegian Environment Agency of NOK 5.7 million (around EUR 500,000) through misuse of the national tax refund scheme for F-gases. Over several years, he had smuggled a total of 3.7 tons of F-gases to Norway and returned the used gas to the refund scheme. By smuggling fluorinated gases into Norway to avoid paying the import tax and returning the containers to the tax refund scheme, he received undue refunds for taxes he had never paid. The man was sentenced to four years and six months' imprisonment. He was also sentenced to pay compensation to the authorities.[77,78]

Photo: Shutterstock

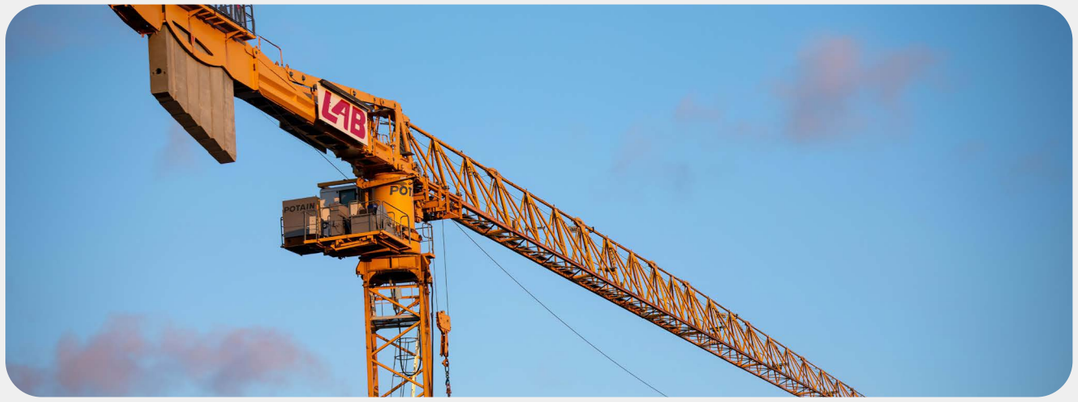


Photo: the police

Use of specialised actors to launder proceeds of crime

Illegally obtained funds must be legitimised before the criminals can spend them. Money laundering is therefore essential to the criminal economy. Crime generates proceeds which can be reinvested in further crimes. Money laundering consequently works as a driver of crime. Over time, money laundering has become professionalised with specialised actors being commissioned to launder money for other criminals. The common denominator of those using their services, is the need to secure proceeds. This makes them completely reliant on the money laundering specialists.

The actors offering money laundering services in Norway have a varying degree of skills and organisation. At entry-level, individual actors offer basic services. As this requires limited skills, there are many such service providers to choose from. At the next level, there are actors and networks with contacts and partners in legal and illegal operations, including in other countries. These function as intermediaries for other money laundering actors. At the top are organised networks that offer laundering of large amounts of proceeds. Such amounts tend to require professionalised services and more complex methods, such as the exploitation of legal company structures or trading in goods and services on the international market, so-called trade-based money laundering.

UNDERGROUND BANKING

Specialised money laundering actors provide a number of unregulated financial services such as the conversion of cash to cryptocurrency, money courier services and money transfers through informal payment systems. When done systematically, this is called *underground banking*[ix], and contributes to facilitating a parallel financial underworld for criminals.[79]

MONEY LAUNDERING THROUGH PROPERTY TRADING

Norway is a country with high property prices and laws that make hidden ownership possible. This provides room for manoeuvre for criminals wishing to launder money through property transactions. Through shell companies and go-betweens, criminal networks invest proceeds of crime in property, and their profits grow at the rate of property prices.

[ix] Sometimes referred to as *informal value transfer systems (IVTS).*

Insiders facilitate crime

Criminals' use of insiders is a serious challenge for private and public sector organisations alike. Many organisations have strengthened their digital defences.[80] This makes it particularly interesting for criminals to build relationships with individuals within organisations. Insider activities contribute to undermining society's trust in institutions and systems, and drains the public purse.

Criminals can make use of insiders to access or change sensitive data. For example, access to sensitive data about security procedures or the possibility to manipulate or falsify documents, can be crucial to actors seeking to commit or continue to commit organised crime. Insiders may also be exploited to sabotage important processes or conceal crimes.[81]

The extent of criminals' use of insiders in Norway is uncertain. Information about insiders may harm the reputation of businesses who are affected by the problem. The propensity to report is low, and the matters are generally handled internally in the organisation. There is, however, a lot to indicate that insider activities are more widespread than what has been documented in publicly available statistics and reporting.[82]

The banking and finance sector is an industry that is particularly exposed to insider activities.[83] A number of finance sector employees have in recent years been under investigation for offences related to insider activities. The increased focus on suspicious transactions and digital security in the banking sector combined with the criminals' need to launder their proceeds, have made insiders particularly valuable for criminals. Insiders can for example facilitate illicit bank loans, and assist with document forgery and the disguising of financial transactions. Improper loans can also be used as a money laundering method whereby proceeds of crime are used to reimburse the loan. Criminal funds are consequently integrated into the legal economy without any economic loss on the part of the bank.

The police have seen a number of such examples of collaborations between bank staff, financial advisers and estate agents. This kind of insider activity can for example be carried out by real estate agents referring clients to financial advisers who can facilitate the grant of improper loans. Moreover, some estate agents also offer to make illegal changes to documents, for example by forging digital valuations, possibly against payment. The police have also seen examples of estate agents who refer clients to one or more named bank staff, who in turn will "assist" them and help them obtain a home loan on a fraudulent basis. Such cooperation may increase the operational leeway for illegal activities.

Insiders in legal organisations assisting criminals is an international problem. Just to mention one example, criminal networks can use insiders to carry out drug smuggling operations outside the scrutiny of customs and border control services. Internationally this has been referred to as the wide-spread criminal infiltration of global cargo supply chains.[84]

Experience from Sweden shows that organised criminals work systematically to recruit insiders in a number of different sectors, including banking and the law enforcement and justice sectors. It also shows that there is a constant flow of supply and demand for the services insiders can provide.[85]

WHAT IS AN INSIDER?

The term insider is here taken to mean a current or previous employee, consultant or contractor who has or has had legitimate access to the organisations' systems, procedures, objects and data, and who misuses their knowledge and access to carry out actions that may harm or cause a loss to the organisation. An insider can be motivated by the desire for profit, but can also act out of loyalty to their family, friends or neighbours, or as a result of pressure, threats or violence. It can also be a combination of these.

A distinction can be made between insiders who deliberately misuse their position, and those who unconsciously contribute to providing access to sensitive information and processes to unauthorised persons. According to the Norwegian National Security Authority, the latter may result from a lack of awareness of security, confidentiality and procedures.[86]

3.3

CYBERCRIME AND ONLINE-BASED CRIMINAL COMMUNITIES

Cybercrime is a persistent threat to the assets and values of our society and a massive challenge to tackle. Every day, society faces attacks on computer systems and malicious digital interaction, with potentially serious consequences for digital and physical values and assets. The number of such attacks has risen over the past few years, in Norway as in the rest of Europe, and this trend is expected to continue.[87,88]

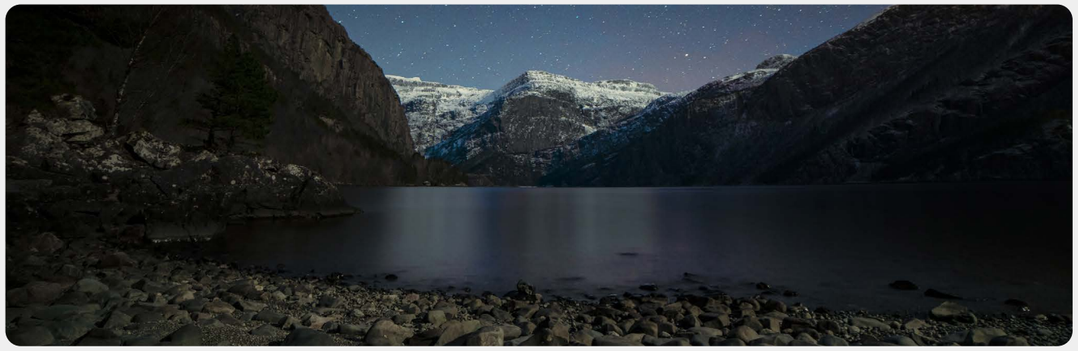
"The rapid digitalisation of everyday life has resulted in the increased complexity of most digital infrastructures. Combined with the speed of transition and the insufficient digital literacy of the broader user base, this has left more systems exposed and vulnerable to cyber-attacks. The increase in cyber-attacks is further driven by the development of more sophisticated tools and techniques available in the Cybercrime-as-a-Service (CaaS) market."

Europol, Serious and organised crime threat assessment 2025[89]

The lines between physical and digital spaces are blurring. Today many types of crime can be committed without the victim, perpetrator or collaborators ever meeting in person. Over the past year, police have gained more insight into various types of criminal online communities. In many of them, a sense of community and belonging is built through a distinct internal culture and a dynamic where boundaries are constantly being pushed. Members often seek to increase their status internally and outperform each other within their criminal niche of choice.

Such digital communities provide more actors with the opportunity to carry out crimes for which they would not otherwise have the necessary skills or room for manoeuvre. This may for example happen through the sharing of knowledge and methods or the hiring of services and technical infrastructure.

> *Digital communities provide more actors with the opportunity to carry out crimes for which they would not otherwise have the necessary skills or room for manoeuvre.*



The Bremanger dam in Vestland county, western Norway, was targeted by a cyberattack, which resulted in the sluice gates being left wide open for several hours. Photo: Shutterstock

Technological vulnerabilities exploited for criminal purposes

A key concern of the police is that cyber-dependent crime may be used to harm technology that controls physical processes, such as the railway network or power grid, so-called *operational technology* (OT). The investigations undertaken by Norwegian police in 2025 included matters where cybercriminals had targeted such OT, some of them fundamental national assets and critical infrastructure.[90,91]

Many legacy systems were developed for safe and stable long-term operation where security was safe-guarded by isolating the system from the organisation's online IT systems. However, due to the need for effective control and supervision, technology used to control physical processes has increasingly been connected to the internet. Generally referred to as cyber-physical connections, these connections result in a new and constantly expanding vulnerability surface.

Most Norwegian businesses and organisations use off-the shelf software from external providers, also in the case of cyber-physical connections to OT systems. In many respects, such standardisation can increase security. But at the same time, consequences can be dire when vulnerabilities emerge. Over the past year, there have been several examples of cybercriminals exploiting so-called *zero-day vulnerabilities* to gain unauthorised access to computer systems. This means that a vulnerability that has yet to be detected by the developers or users of the IT system, is exploited by a threat actor seeking to gain unauthorised access.

ZERO-DAY VULNERABILITIES

I 2025 hackers exploited a zero-day vulnerability in Microsoft SharePoint before Microsoft had had the chance to patch it. The vulnerability enabled attackers to access to computer systems used by a vast number of organisations to store and share information. As the vulnerability was unknown both to Microsoft and the users when the attack was launched, they had zero days to correct it, hence the name zero-day vulnerability. Before a new patch removing the vulnerability could be released, hackers exploited and attempted to gain access to systems belonging to large public and private sector organisations.[92]

The electric buses used by the public transport provider Ruter contain "backdoor" technology making it possible to remote control them. Whilst it is uncertain whether this is an intended feature, it constitutes a major vulnerability.[101]
Photo: Eilif Swensen/Ruter

Ideologically motivated *hacktivism* is a persistent threat facing Norway.[93] In April 2025, a pro-Russian group hacked into the control systems of a water dam in Bremanger. This is an example of an ideologically motivated attack on OT systems in Norway.[94]

Over the past few years, there have also been numerous examples of so-called *supply chain attacks*[x,96,97,98,99] This is where technical backdoors are built into hardware components or firmware. Vulnerabilities of this type can be particularly hard to detect and remove as they are often located in a part of the device that neither end-users nor anti-virus applications have access to.[100] There is also a risk that they can be detected and exploited by others than those originally creating the backdoor. Both zero-day vulnerabilities and supply chain attacks significantly increase the potential to harm Norwegian targets as many of the organisations managing important assets use the same type of IT infrastructure.

HACKTIVISM

Hacktivism combines politically or ideologically motivated activism with cybercrime and constitutes a persistent threat to Norwegian values, assets and interests. This is a wider concept than denial-of-service attacks, which also includes information and data theft, data leaks and distribution of stolen data as well as other politically or ideologically motivated digital crimes.[95]

[x] Also known as *value-chain attacks* or *backdoor breaches*.

Changing target selection processes

Cyber-dependent crimes are many and diverse. The actor landscape is complex covering a wide array of roles springing from various practical needs in the chain of attack. In this ecosystem there is a large number of inexperienced and less competent actors who identify targets and obtain results through, amongst other things, entry-level use of AI and commercially available software tools.

However, at the other end of the scale, targeted customised attacks committed by a small group of professional cybercriminals against carefully selected victims is another international trend. This is due to the fact that a single successful attack against a high-value target can generate high profits that can justify significant investments prior to the attack. An attack is a process consisting of a number of stages in which some roles can be outsourced to external experts.[102] This is a type of *crime-as-a-service*, as described in chapter 3.1.

A computer intrusion does not only present a threat to the target at the time of the attack, it can also facilitate future attacks through use of the stolen data. The police and other partner organisations regularly see examples of cybercriminals exploiting assets from previous computer intrusions to select and gain access to new targets.[103,104,105,106,107]

The gateway to the carefully selected target is often a so-called *initial access broker*[xi]. This refers to a specialised cybercriminal offering advice on which organisations to target and selling stolen credentials for their computer systems. When targets are selected by specialised criminals, other cybercriminals can focus their efforts on carrying out the attack.[108] The initial access broker works continuously to obtain login details or credentials through methods such as phishing[xii] targeting big email databases, or through malicious websites. This involves "casting a wide net" to catch as many internet users as possible. The initial access broker can then either sell credentials (user names and passwords) to others or obtain access by installing malware that connects the user's computer to a network of remotely controlled devices, often referred to as a *botnet*. This way, the initial access broker maintains a list of potential targets characterised by low security and high value. Other professional cybercriminals can purchase this information and exploit it to attack targets likely to generate a profit.

In addition to initial access brokers, there are also specialised *data brokers*[xiii]. These offer valuable data retrieved from the victim's computer systems for sale. Over the past few years, data have increasingly been considered an independent commodity that can be sold on to various interested parties.[109,110] In the police's experience, the different brokers by and large use the same techniques and can take on several roles in parallel.

Photo: the police

[xi] Sometimes shortened to *IAB*.
[xii] For example by the initial access broker sending a mass email urging the recipient to click on a malicious link or download an attachment.
[xiii] Also referred to as *information brokers (IB)*.

THE DARK WEB

CRIMINALS EXCHANGE SERVICES, DATA AND TOOLS ON THE DARK WEB

Cybercriminals take a number of different measures to hide their identity and cover their traces, including any links to other actors. It has gradually become safer for criminals to use commercially available solutions, as service providers are increasingly security-minded and offer robust end-to-end encryption of their messaging applications as default.

Nevertheless, many actors go one step further and use a part of the internet that is hidden from ordinary search engines and indexing services. This is known as *the dark web*. User interfaces and features are very similar to the open web, but special web browsers are often required. The best-known example of a browser providing access to the dark web is The Onion Router (TOR). In the police's experience, a large proportion of cybercriminals exchange experiences, methods and tools on dedicated forums and marketplaces on the dark web. Criminal projects are organised and new resources recruited or hired in these digital communities.

Both supply and demand for crime-as-a-service are particularly high within areas such as ransomware and other kinds of extortion in the wake of computer intrusions. Artificial intelligence is pressuring prices of many digital goods and services on criminal marketplaces, including zero-day vulnerabilities and phishing services.

Police Threat Assessment 2026 – Norway Section 03 Contents

BANDITS ILLEGAL REQUIREMENTS FORUM

Bandits Illegal Requirements Forum is an arena for collaboration on the dark web. The forum is a meeting place for actors committing cybercrime or offering support services for such activities. Although there are few rules, a small number of administrators oversee the forum and carry out some degree of content moderation. These are based in countries with which Norway has no functioning law enforcement cooperation or extradition treaty. Access to the forum is subject to a number of authentication steps including a video call and an interview. A monthly membership fee of USD 300 is payable in cryptocurrency.

The online community has a number of sub-forums for various topics including methods, target types and programming languages. A number of applications and uses are covered ranging from the sharing of experience, identification of unreliable actors and sale of data obtained through illegal methods, to coding discussions. Added together, this provides criminal actors operating in the cyber-domain with pretty nearly everything they can wish for, including social interaction with like-minded people.

Bandits Illegal Requirements Forum is a fictitious example based on the police's knowledge of and access to similar digital forums. Fictionalisation is required to protect the police's work and use of covert methods.

Photo: Shutterstock

Extreme web communities manipulate and inflict harm on vulnerable young people

Norwegian police and international partner organisations have over the past few years gained insight into a number of online communities and groups cultivating violence in the extreme. The members of these forums inflict serious physical and psychological harm on young children and teenagers through cynical and targeted manipulation and extortion. As opposed to many other types of crime, the primary motive is neither sex nor financial gain. The acts are driven by a desire for power, thrills and recognition in closed online forums where violence, denigration and misogyny give a high status. Inside these online forums, members are gradually desensitised to graphic descriptions of grotesque violence and sexual acts. The coaxing process is driven by the frequent sharing of violent material by users seeking to outperform each other.

The online communities vary in size, but some of them have several thousand members.[111] The police are actively seeking to identify victims and offenders. Although only a small number of persons with links to this phenomenon have been identified in Norway, unrecorded numbers are thought to be high. As victims perform increasingly extreme acts, they are often left with a strong feeling of shame and it becomes increasingly hard to break out of the circle or seek help.

The purpose of these extreme online communities is to inflict as much harm as possible on the victims and their surroundings through manipulation and pressure. A typical method is to build a relation to a young person showing signs of vulnerability, playing on shared experiences and romantic feelings in the communication.

In the first stage, there is an abundance of positive feedback and expressions of love in various forms. The aim is to make the victim share explicit images of themselves or details from their life that they want to keep from falling into the wrong hands. Once one or more potential means of extortion have been established, the tone changes: The perpetrator plays on established feelings whilst at the same time threatening to share what the victim perceives as revealing material. The victim is gradually pressured into taking part in increasingly hard challenges. This can for example be self-harming by scratching the manipulator's username into their own skin, masturbating using a knife or cactus, burning their skin, raping a family member or torturing their own pet.

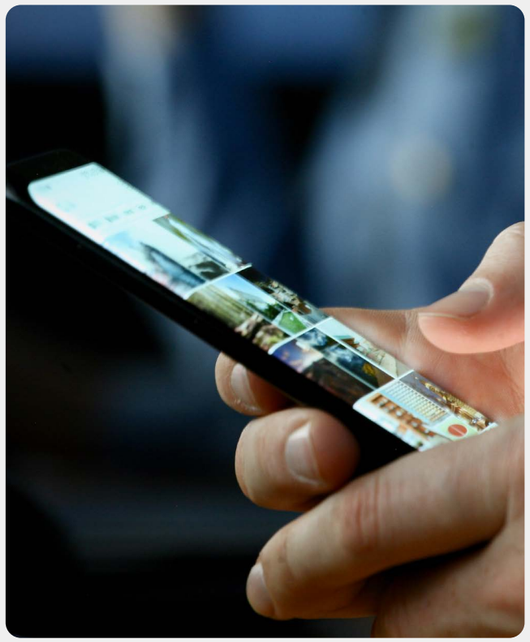


Photo: the police

The communication and the acts carried out by the victim are recorded in video and photos. The material is shared liberally with the other members to achieve a high status in the group and receive advice on what to do next with the victim. The purpose is to break down the victim mentally and make them ruin their life to the extent that they commit suicide live online.

Data available to the police show a certain overlap between the groups, whose members and victims are based in a number of different countries. Although some of the involved are up to 25 years old, the perpetrators are largely boys aged 14–17. The victims are generally a few years younger than their manipulators, and almost exclusively girls. Victims are sometimes pressured into finding new victims themselves and exposing them to a similar process.

THE 764 ONLINE COMMUNITY

One publicly known example of such an online community is "764", founded in 2021 by Bradley Cadenhead, who was 15 years old at the time. The expressed purpose of the community was to destabilise society by changing the attitudes of youngsters' in a destructive direction. This was going to happen through the normalisation of graphic content, the breaking down of established norms and the destruction of young people's ethics. Leading figures posted guidelines on how to identify suitable victims, one of them being to seek out users on "self-harm forums". In 2023, Cadenhead was convicted and sentenced to 80 years' imprisonment in the USA for his activities[112], and in 2025, two other leading members of the group were arrested and indicted.[113]

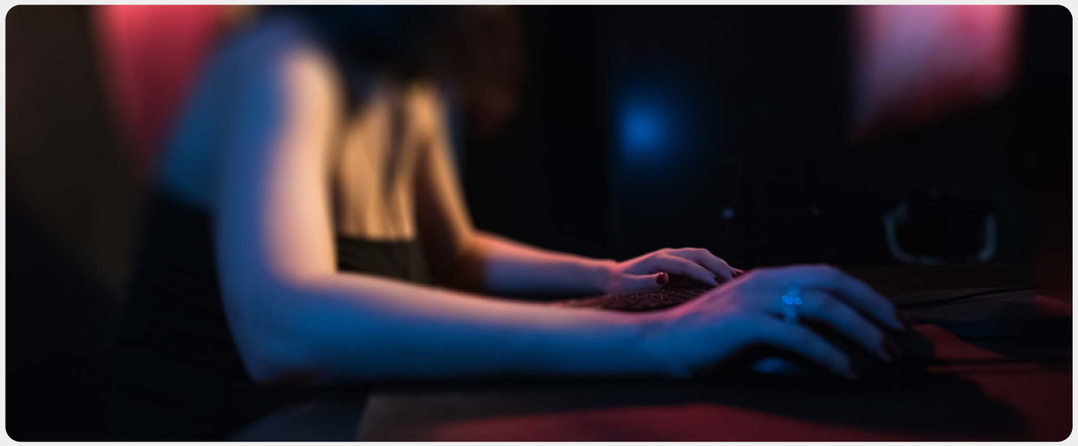


Photo: Shutterstock

REFERENCES

1. Norwegian Parliament 2025. *Parliamentary White Paper no. 20: Innsats for demokrati, rettsstat og menneskerettigheter i Europa Norges arbeid i Europarådet.* Retrieved from: https://www.regjeringen.no/no/dokumenter/meld.-st.-20-20242025/id3095394/
2. Information from the latest threat assessments by the Norwegian Police Security Service and the Norwegian Intelligence Service. See: Police Security Service. 2026. *Nasjonal trusselvurdering 2026.* Retrieved from: https://www.pst.no/trusselbilde/norsk-trusselvurdering/; and the Norwegian Intelligence Service. (2026). *Fokus 2026.* Retrieved from: https://www.etterretningstjenesten.no/publikasjoner/fokus
3. Definition used by the intelligence and security services. See: Police Security Service. 2026. *Nasjonal trusselvurdering 2026.* Retrieved from: https://www.pst.no/trusselbilde/norsk-trusselvurdering/ ; Norwegian Intelligence Service. (2026). *Fokus 2026.* Retrieved from: https://www.etterretningstjenesten.no/publikasjoner/fokus; and Norwegian National Security Authority (2026). Risiko 2026. Retrieved from: https://nsm.no/aktuelt/risiko-2026
4. Lovdata. 1998. *Agreement between Norway and Russia on cooperation in combating crime* Retrieved from: https://lovdata.no/dokument/TRAKTAT/traktat/1998-05-26-4
5. Egmont Group. 2013. *Egmont Group Charter.* Retrieved from: https://egmontgroup.org/wp-content/uploads/2021/09/Egmont-Group-Charter-Revised-July-2023-Abu-Dhabi-UAE.pdf
6. Interpol. 1956. *Constitution of the ICPO-Interpol (updated 2023).* Retrieved from: https://www.interpol.int/Who-we-are/Legal-framework/Legal-documents
7. National Police Directorate. 2025. *Norsk politi har inngått intensjonsavtale med Marokko.* Retrieved from: https://www.politiet.no/nyheter-og-presse/politidirektoratet/nyhet/2025-11-26/norsk-politi-har-inngatt-intensjonsavtale-med-marokko?nyhetsmelding=0
8. Ministry of Finance. 2025. *Parliamentary White Paper no. 31, Perspektivmeldingen 2024.* Retrieved from: https://www.regjeringen.no/no/dokumenter/meld.-st.-31-20232024/id3049290/
9. Ministry of Finance. 2025. *Parliamentary White Paper no. 31, Perspektivmeldingen 2024.* Retrieved from: https://www.regjeringen.no/no/dokumenter/meld.-st.-31-20232024/id3049290/
10. Norsk Eiendom. 2025. *Hvitvasking i eiendomsbransjen: 100 milliarder i spill, og vi ser ikke hvem som eier.* Retrieved from: https://www.norskeiendom.org/aktuelt/nyheter/hvitvasking-i-eiendomsbransjen---100-milliarder-i-spill-og-vi-ser-ikke-hvem-som-eier
11. Central Bank of Norway. 2025. *Monetary policy report 2/2025.* Retrieved from: https://www.norges-bank.no/en/news-events/publications/Monetary-Policy-Report/2025/mpr-22025/web-report-mpr-22025/
12. Norwegian Broadcasting Corporation (NRK). 2024. *Vipps om ranene – Vanskelig å stoppe.* Retrieved from: https://www.nrk.no/stor-oslo/vipps-om-ranene_-_-vanskelig-a-stoppe-1.16908285
13. Norwegian Defence Research Establishment (FFI) 2021. *Samfunnsutvikling frem mot 2030 – Utfordringer for politiet, PST og påtalemyndigheten. (FFI report 21/01132).* Retrieved from: https://www.ffi.no/publikasjoner/arkiv/samfunnsutvikling-frem-mot-2030-utfordringer-for-politiet-pst-og-patalemyndigheten
14. National Criminal Investigation Service 2024. *Barn som selger egenprodusert seksualisert materiale til voksne: En beskrivelse av fenomenet og omfanget (Version 2.0/2024).* Retrieved from: https://www.politiet.no/globalassets/dokumenter-strategier-og-horinger/kripos/seksuelle-overgrep/barn-som-selger-egenprodusert-seksualisert-materiale-til-voksne.pdf
15. Police. 2025. *Barne- og ungdomskriminaliteten i Oslo: Basert på data fra 2024.* Retrieved from: https://www.politiet.no/globalassets/dokumenter-strategier-og-horinger/oslo/rapporter/barne--og-ungdomskriminalitet/barne--og-ungdomskriminaliteten-i-oslo-2024.pdf
16. Director of Public Prosecutions. 2025. *Prioriteringer for straffesaksbehandlingen i 2025.* Retrieved from: https://www.riksadvokaten.no/document/prioritering-ar-for-straffesaksbehandlinga-2025/
17. National Police Directorate and Director of Public Prosecutions. 2025. *Straffesaksbehandlingen i politiet 2024.* Retrieved from: https://www.riksadvokaten.no/wp-content/uploads/2025/03/Straffesaksbehandlingen-i-politiet-2024.pdf
18. Director of Public Prosecutions. 2023. *Circular 2/2023. Om vold i nære relasjoner.* Retrieved from: https://www.riksadvokaten.no/wp-content/uploads/2024/12/Rundskriv-2-2023-vold-i-naere-relasjoner.pdf
19. Norwegian Penal Code section 57, see also https://www.domstol.no/no/straffesak/straffesaker-under-etterforskning/besoksforbud/ and https://www.politiet.no/rad/vold-i-nare-relasjoner/voldsalarm-og-omvendt-voldsalarm for more information
20. National Police Directorate and Director of Public Prosecutions. 2025. *Straffesaksbehandlingen i politiet 2024.* Retrieved from: https://www.riksadvokaten.no/wp-content/uploads/2025/03/Straffesaksbehandlingen-i-politiet-2024.pdf
21. Police. 2025. *Statistikk for bruk av omvendt voldsalarm.* Retrieved from: https://www.politiet.no/om-politiet/tall-og-fakta/mobil-omvendt-voldsalarm
22. National Criminal Investigation Service. 2026. *Nasjonal drapsoversikt 2025.* Retrieved from: https://edit.politiet.no/globalassets/tall-og-fakta/drap/nasjonal-drapsoversikt-2025.pdf
23. National Criminal Investigation Service. 2026. *Nasjonal drapsoversikt 2025.* Retrieved from: https://edit.politiet.no/globalassets/tall-og-fakta/drap/nasjonal-drapsoversikt-2025.pdf
24. National Criminal Investigation Service. 2026. *Nasjonal drapsoversikt 2025.* Retrieved from: https://edit.politiet.no/globalassets/tall-og-fakta/drap/nasjonal-drapsoversikt-2025.pdf
25. Norwegian Government. 2025. *I dag trer samtykkeloven i kraft.* Retrieved from: https://www.regjeringen.no/no/aktuelt/i-dag-trer-samtykkeloven-i-kraft/id3113434/
26. National Criminal Investigation Service. 2025. *Seksuell utpressing med økonomisk motiv.* Retrieved from: https://www.politiet.no/globalassets/tall-og-fakta/seksuelle-overgrep-mot-barn/seksuell-utpressing-med-okonomisk-motiv.pdf
27. National Criminal Investigation Service. 2024. *Barn som selger egenprodusert seksualisert materiale til voksne: En beskrivelse av fenomenet og omfanget.* Retrieved from: https://www.politiet.no/globalassets/dokumenter-strategier-og-horinger/kripos/seksuelle-overgrep/barn-som-selger-egenprodusert-seksualisert-materiale-til-voksne.pdf
28. Director of Public Prosecutions. 2021. *Circular – Påtalemyndighetens legalitetskontroll med tvangsmiddelbruk – Relevant etterforskningsformål og forholdsmessighet. Særlig om ransaking i narkotikasaker.* Retrieved from: https://www.riksadvokaten.no/document/patalemyndighetens-legalitetskontroll-med-tvangsmiddelbruk/
29. National Criminal Investigation Service. 2026. Narkotikastatistikk 2025. Retrieved from: https://www.politiet.no/globalassets/tall-og-fakta/narkotika/narkotikastatistikk-2025.pdf
30. Samfunnsøkonomisk analyse. 2025. *Kartlegging av virksomheters og kommuners utsatthet for økonomisk kriminalitet. Report no. 35-2025.* Retrieved from: https://samfunnsokonomisk-analyse.no/publikasjoner/kartlegging-av-virksomheters-og-kom-

muners-utsatthet-for-okonomisk-kriminalitet-2025
31. Samfunnsøkonomisk analyse. 2025. *Kartlegging av virksomheters og kommuners utsatthet for økonomisk kriminalitet. Report no. 35-2025.* Retrieved from: https://samfunnsokonomisk-analyse.no/publikasjoner/kartlegging-av-virksomheters-og-kommuners-utsatthet-for-okonomisk-kriminalitet-2025
32. Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim). 2025. *Beregnet utbytte fra bedragerier i Norge 2024.* Retrieved from: https://kudos.dfo.no/documents/398479/files/48156.pdf
33. Transparency International. 2025. *Global corruption Index score 81. (Ranking 4 out of 182 countries.)* Retrieved from: https://www.transparency.org/en/countries/norway
34. The European Union Agency for Cybersecurity. 2025. *Enisa threat landscape 2025.* Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
35. Næringslivets sikkerhetsråd. 2025. *Mørketallsundersøkelsen 2024.* Retrieved from: https://www.nsr-org.no/aktuelt/morketallsundersokelsen-2024
36. Nätt T. H. & Bartnes, M. 2025. *Tjenestenekt*. Retrieved from: https://snl.no/tjenestenekt
37. National Cybercrime Centre / NC3. 2026. Cyberkriminalitet 2026. Pending publication.
38. Koordineringsenheten mot menneskehandel. 2025. *Tilstandsrapport 2024*
39. UNODC. 2008. *An introduction to human trafficking.* Retrieved from: https://www.unodc.org/documents/human-trafficking/An_Introduction_to_Human_Trafficking_-_Background_Paper.pdf
40. UNODC. 2009. *Prevention of human trafficking.* Retrieved from: https://www.unodc.org/southasia/en/topics/frontpage/2009/preventin-of-human-trafficking.html
41. Norwegian Government. 2025. *Nasjonal strategi mot menneskehandel (2025 - 2030)* Retrieved from: https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-mot-menneskehandel-2025-2030/id3103576/
42. Norwegian Government. 2025. *Nasjonal strategi mot menneskehandel (2025 - 2030)* Retrieved from: https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-mot-menneskehandel-2025-2030/id3103576/
43. National Criminal Investigation Service. 2025. *Trender innen menneskehandel 2024.*
44. Europol. 2025. *The changing DNA of serious and organised crime. EU Serious and Organised Threat Assessment (SOCTA).* Retrieved from: https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime
45. Europol. 2025. *The changing DNA of serious and organised crime. EU Serious and Organised Threat Assessment (SOCTA).* Retrieved from: https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime
46. Europol. 2025. *The changing DNA of serious and organised crime. EU Serious and Organised Threat Assessment (SOCTA).* Retrieved from: https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime
47. OsloMet NOVA. 2025. *Results from the Ungdata-undersøkelsen 2025 survey.* Retrieved from: https://www.ungdata.no/rapporter/
48. OsloMet NOVA. 2025. *Results from the Ungdata-undersøkelsen 2025 survey.* Retrieved from: https://www.ungdata.no/rapporter/
49. Norwegian Institute of Public Health. 2018. *Skader og problemer knyttet til narkotikabruk*. https://www.fhi.no/le/rusmidler-og-avhengighet/narkotikainorge/konsekvenser-av-narkotikabruk/skader-og-problemer-knyttet-til-narkotikabruk
50. Norwegian Institute of Public Health. 2025. *Narkotikautløste dødsfall i Norge.* Retrieved from: https://www.helsedirektoratet.no/tema/narkotikautloste-dodsfall-i-norge
51. Norwegian Institute of Public Health. 2025. *Narkotikautløste dødsfall i Norge.* Retrieved from: https://www.helsedirektoratet.no/tema/narkotikautloste-dodsfall-i-norge
52. European Commission, RUSI and GI-TOC. 2025. *MASIF - Evaluating Cocaine Market Interventions: How External Shocks and Disruption of Criminal Networks Impact the Cocaine Trade and Social Outcomes.*
53. Europol. 2025. *The changing DNA of serious and organised crime. EU Serious and Organised Threat Assessment (SOCTA).* Retrieved from: https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime
54. Europol. 2025. *The changing DNA of serious and organised crime. EU Serious and Organised Threat Assessment (SOCTA).* Retrieved from: https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime
55. National Criminal Investigation Service. 2025. *Vold som handelsvare*. Retrieved from: https://www.politiet.no/globalassets/tall-og-fakta/kriminelle-nettverk/2025-10-16-a-vold-som-handelsvare---kripos_.pdf
56. Europol. 2025. *The changing DNA of serious and organised crime. EU Serious and Organised Threat Assessment (SOCTA).* Retrieved from: https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime
57. VG. 2025. *Kripos: Har avdekket 400 voldsoppdrag hittil i år.* Retrieved from: https://www.vg.no/nyheter/i/e71We4/kripos-400-avdekkede-og-30-avvergede-voldsoppdrag-i-norge
58. National Criminal Investigation Service. 2025. *Trusler mot unge utøvere involvert i voldsoppdrag for kriminelle nettverk.* Retrieved from: https://www.politiet.no/globalassets/tall-og-fakta/kriminelle-nettverk/2025-12-16-a-trusler-mot-unge-utovere-involvert-i-voldsoppdrag-for-kriminelle-nettverk---kripos.pdf
59. National Criminal Investigation Service. 2025. *Vold som handelsvare.* Retrieved from: https://www.politiet.no/globalassets/tall-og-fakta/kriminelle-nettverk/2025-10-16-a-vold-som-handelsvare---kripos_.pdf
60. Samfunnsøkonomisk analyse. 2022. *Samfunnsøkonomiske kostnader av kriminalitet. Report 6–2022*. Retrieved from: https://www.regjeringen.no/contentassets/c1e4467f7fea4adfaf346429cb525b46/r06-2022-samfunnsokonomiske-kostnader-av-kriminalitet.pdf
61. Expertgruppen för Studier i Offentlig ekonomi (ESO). 2026. *Svarta siffror – en ESO-rapport om den kriminella ekonomins omfattning.* Retrieved from: https://eso.expertgrupp.se/wp-content/uploads/2024/10/ESO-rapport-2026_1_svarta-siffror_webb.pdf
62. Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim). 2024. *Nordic threat assessment on online fraud 2024.* Retrieved from: https://www.okokrim.no/nordic-threat-assessment-on-online-fraud-2024.6685282-562360.html
63. Expertgruppen för Studier i Offentlig ekonomi (ESO). 2026. *Svarta siffror – en ESO-rapport om den kriminella ekonomins omfattning.* Retrieved from: https://eso.expertgrupp.se/wp-content/uploads/2024/10/ESO-rapport-2026_1_svarta-siffror_webb.pdf
64. Kibar. 2025. *Skatteetaten og NAV erkjenner at systemene er under press: Manipulerer offentlige registre i økende tempo.* Retrieved from: https://www.dn.no/kriminalitet/skatteetaten-og-nav-erkjenner-at-systemene-er-under-press-manipulerer-offentlige-registre-i-okende-tempo/2-1-1894774.
65. Norwegian Digitalisation Agency (Digdir). 2025. *Hva er en elektronisk identitet (eID)?* Retrieved from: https://www.digdir.no/digital-identitet/hva-er-en-elektronisk-identitet-eid/7310
66. National Joint Analysis and Intelligence Centre (NTAES). 2024. *Registermanipulasjon*. Retrieved from: https://www.ntaes.no/reports/NTAES%20Rapport%20Registermanipulasjon.pdf
67. National Joint Analysis and Intelligence Centre (NTAES). 2024. *Registermanipulasjon*. Retrieved from: https://www.ntaes.no/reports/NTAES%20Rapport%20Registermanipulasjon.pdf
68. EUROPOL. 2025. *IOCTA Steal, deal and repeat; How cybercriminals trade and exploit your data.* Retrieved from: https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data
69. Norwegian Broadcasting Corporation (NRK). 2025. *På innsiden av svindelsentralen.* Retrieved from: https://www.nrk.no/dokumentar/xl/svindelsentralen-1.17333817
70. National Joint Analysis and Intelligence Centre (NTAES). 2024. *Registermanipulasjon*. Retrieved from: https://www.ntaes.no/reports/NTAES%20Rapport%20Registermanipulasjon.pdf

71. National Joint Analysis and Intelligence Centre (NTAES). 2024. *Registermanipulasjon*. Retrieved from: https://www.ntaes.no/reports/NTAES%20Rapport%20Registermanipulasjon.pdf
72. National Joint Analysis and Intelligence Centre (NTAES). 2024. *Registermanipulasjon*. Retrieved from: https://www.ntaes.no/reports/NTAES%20Rapport%20Registermanipulasjon.pdf
73. Norwegian Tax Administration. 2024. *Skatteetaten med 67 mva-anmeldelser.* Retrieved from: https://www.skatteetaten.no/presse/nyhetsrommet/skatteetaten-med-67-mva-anmeldelser-/
74. National Joint Analysis and Intelligence Centre (NTAES). 2024. *Registermanipulasjon*. Retrieved from: https://www.ntaes.no/reports/NTAES%20Rapport%20Registermanipulasjon.pdf
75. KPMG. 2024. *Misbruk av A-ordningen og SBL er et samfunnsproblem.* Retrieved from: https://kpmg.com/no/nb/innsikt/sikkerhet-risiko/misbruk-a-ordningen-sbl.html
76. Norwegian Labour and Welfare Administration (NAV). 2025. *Nav anmeldte trygdesvindel for 76 millioner i fjor.* Retrieved from: https://www.nav.no/no/nav-og-samfunn/statistikk/flere-statistikkomrader/nyheter/nav-anmeldte-trygdesvindel-for-76-millioner-i-fjor
77. Borgarting Court of Appeal, judgment of 7 December 2023 in case LB-2023-75834.
78. Borgarting Court of Appeal, judgment of 8 March 2024 in case LB-2023-177824.
79. Europol. 2025. *The changing DNA of serious and organised crime. EU Serious and Organised Threat Assessment (SOCTA).* Retrieved from: https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime
80. The Norwegian Financial Services Authority 2025. *Risiko- og sårbarhetsananlyse 2025.* Retrieved from: https://www.finanstilsynet.no/publikasjoner-og-analyser/risiko--og-sarbarhetsanalyse/risiko--og-sarbarhetsanalyse-2025/
81. Norwegian National Security Authority. 2020. *Topical report: Innsiderisiko*. Retrieved from: https://nsm.no/getfile.php/133153-1591706148/NSM/Filer/Dokumenter/Rapporter/Temarapport%20innsidere.pdf
82. KPMG. 2025. *Innsiderisiko. Dybdeundersøkelse om økonomisk kriminalitet og innsidetrusselen.* Retrieved from: https://assets.kpmg.com/content/dam/kpmgsites/no/pdf/cyber-security/kpmg-dybdeundersokelse-om-innsiderisiko.pdf.coredownload.inline.pdf
83. Central Bank of Norway. 2020. *Hvitvasking og det finansielle systemet*. Retrieved from: https://www.norges-bank.no/bankplassen/arkiv/2020/hvitvasking-og-det-finansielle-systemet/
84. World Customs Organization. 2024. *Infiltration of maritime cargo supply chains. Organized crime, cocaine and the internal conspirator.* Retrieved from: https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/enforcement-and-compliance/activities-and-programmes/sci-project/wco-report_infiltration-of-maritime-cargo-supply-chains_june-2025.pdf
85. Brå. 2024. *Möliggörare för kriminella nätverk. Rapport 2024-2.* Retrieved from: https://bra.se/rapporter/arkiv/2024-03-01-mojliggorare-for-kriminella-natverk
86. Norwegian National Security Authority. 2020. Topical report: Innsiderisiko. Retrieved from: https://nsm.no/getfile.php/133153-1591706148/NSM/Filer/Dokumenter/Rapporter/Temarapport%20innsidere.pdf
87. European Union Agency for Cybersecurity. 2024. *ENISA Threat Landscape 2024*. Retrieved from: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf
88. National Criminal Investigation Service. 2026. *Cyberkriminalitet 2026*. Pending publication.
89. Europol. 2025. *The changing DNA of serious and organised crime. EU Serious and Organised Threat Assessment (SOCTA).* Retrieved from: https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime
90. National Criminal Investigation Service. 2026. *Cyberkriminalitet 2026*. Pending publication.
91. National Criminal Investigation Service. 2025. *Cyberkriminalitet 2025*. Retrieved from: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2025.pdf
92. The main vulnerabilities were named CVE-2025-53770 and CVE-2025-53771. See e.g. CISA. 2025. *CISA releases malware analysis report associated with Microsoft Sharepoint vulnerabilities.* Retrieved from: https://www.cisa.gov/news-events/alerts/2025/08/06/cisa-releases-malware-analysis-report-associated-microsoft-sharepoint-vulnerabilities
93. National Criminal Investigation Service. 2026. *Cyberkriminalitet 2026*. Pending publication.
94. Norwegian Broadcasting Corporation (NRK). 2025. *PST mener prorussiske hackere stod bak sabotasje – henlegger likevel saken.* Retrieved from: https://www.nrk.no/vestland/pst-mener-prorussisk-hackergruppe-stod-bak-dam-sabotasje-pa-vestland-et-og-datainnbrudd-pa-ostlandet-1.17587446
95. National Criminal Investigation Service. 2026. *Cyberkriminalitet 2026*. Pending publication.
96. Leyden, John. 2017. *Malware 'disguised as Siemens software drills into 10 industrial plants'*. Retrieved from: https://www.theregister.com/2017/03/22/malware_siemens_plc_firmware/
97. Paganini, Pierluigi. 2023. *Android devices shipped with backdoored firmware as part of the BADBOX network*. Retrieved from: https://securityaffairs.com/152124/malware/badbox-network-backdoored-firmware.html
98. KrebsOnSecurity. 2026. *The Kimwolf Botnet is Stalking Your Local Network*. Retrieved from: https://krebsonsecurity.com/2026/01/the-kimwolf-botnet-is-stalking-your-local-network/
99. Police Security Service. 2025. *National threat assessment 2025*. Retrieved from: https://www.pst.no/globalassets/2025/nasjonal-trusselvurdering-2025/nasjonal-trusselvurdering-2025_no_web.pdf
100. Asadoorian, Paul. 2022. *Firmware Attacks: An Endpoint Timeline*. Retrieved from: https://eclypsium.com/blog/endpoint-firmware-attack-timeline-introduction/
101. Norwegian Broadcasting Corporation (NRK). 2025. *Ruters egne tester viser: Oslo-elbusser kan stoppes og slås av fra Kina.* Retrieved from: https://www.nrk.no/stor-oslo/ruters-egne-tester-viser_-oslos-elbusser-kan-fjernstyres-1.17629321
102. National Criminal Investigation Service. 2026. *Cyberkriminalitet 2026*. Pending publication.
103. Cyberint. 2025. *Initial Access Brokers Report*. Retrieved from: https://e.cyberint.com/hubfs/IAB%20Report%202025.pdf
104. Hoxhunt. 2024. *Phishing Trends Report (updated for 2025)*. Retrieved from: https://hoxhunt.com/guide/phishing-trends-report
105. Khalil, Mohammed. 2025. *Supply chain attack statistics 2025: Costs, cases, defenses.* Retrieved from: https://deepstrike.io/blog/supply-chain-attack-statistics-2025
106. Reversing labs. 2025. *The 2025 software supply chain security report: Attacks grow in sophistication – targeting AI, crypto, open source, and commercial software*. Retrieved from: https://ntsc.org/wp-content/uploads/2025/03/The-2025-Software-Supply-Chain-Security-Report-RL-compressed.pdf
107. National Criminal Investigation Service. 2025. *Cyberkriminalitet 2025*. Retrieved from: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2025.pdf
108. National Criminal Investigation Service. 2025. *Cyberkriminalitet 2025*. Retrieved from: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2025.pdf
109. Infostealers by HudsonRock. 2025. *The Infostealer-to-APT Pipeline: How Stolen Diplomatic Credentials Fuel Cyber-Political Power Plays.* Retrieved from: https://www.infostealers.com/article/the-infostealer-to-apt-pipeline-how-stolen-diplomatic-credentials-fuel-cyber-political-power-plays/
110. National Criminal Investigation Service. 2025. *Cyberkriminalitet 2025*. Retrieved from: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2025.pdf
111. FBI USA. 2025. *Public service announcement. The com: theft, extortion and violence are a rising threat to youth online.* Retrieved from: https://www.ic3.gov/PSA/2025/PSA250723-3#fn5
112. Texas departement of criminal justice. 2025. *Inmate information details. Displays the maximum sentence date 01.12.2102.* Retrieved from: https://inmate.tdcj.texas.gov/InmateSearch/viewDetail.action?sid=19984471
113. FBI USA. 2025. *Criminal Complaint in case 1:25-mj-00061-ZMF (United States District Court for the District of Columbia).* Retrieved from: https://www.justice.gov/usao-dc/media/1398431/dl

Police Threat Assessment 2026 – Norway References Contents

TIP-OFFS TO THE POLICE

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 tip-off line on **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**

SELECTED SUPPORT SERVICES

If you need help, but do not want to contact the police, there are a number of other options.

Did you know that you have a duty to avert offences?
If you have a suspicion of serious violence or abuse, you have a duty to report it. This duty takes precedence over the duty of confidentiality.

→ **Read more on plikt.no.**

Are you a victim of violence or sexual abuse?
Contact the sexual assault referral centre where you live or call the urgent care centre on **116 117.**

→ **Dinutvei.no**

Do you have sexual thoughts and feelings about children?
There is help.

→ **Detfinneshjelp.no**

Do you need someone to talk to?

Mental helse helpline: **116 123**
Kirkens SOS helpline: **22 40 00 40**

POLITIET

Police Threat Assessment 2026

Published by: National Criminal Investigation Service

politiet.no/trusselvurdering

Published on 25 February 2026