THE POLICE

POLICE THREAT ASSESSMENT 2021, NORWAY

NCIS

The Norwegian Police's 2021 Threat Assessment is one of several threat and risk assessments issued by public authorities in the first quarter of each year. Some of the most relevant are mentioned below:

THE POLICE SECURITY SERVICE is Norway's national domestic intelligence and security service, reporting to the Minister of Justice and Public Security. The purpose of the Service is to prevent and investigate serious crime jeopardizing national security. The Service is charged with the identification and assessment of threats which concern intelligence, sabotage, proliferation of weapons of mass destruction, terrorism and extremism. Their assessments are intended to inform the shaping of policies and support decision-making processes. The annual threat assessment of the Police Security Service is part of the Service's public communication, setting out anticipated developments of the threat picture.

THE NATIONAL SECURITY AUTHORITY is Norway's specialist authority for preventive national security. The Directorate advises on and conducts inspections and other supervisory activities related to the protection of information, systems, potential targets and infrastructure of national importance. The Authority also holds national responsibility for detecting, alerting to and coordinating the handling of serious ICT attacks. The Risk Report is the Authority's annual assessment of the risk picture regarding national security. The report assesses how vulnerabilities in Norwegian enterprises and important services impact the risk picture, in light of the threat picture as assessed by the Norwegian Intelligence Service and the Police Security Service. It also recommends measures to mitigate risk associated with activity which threatens security.

THE INTELLIGENCE SERVICE is Norway's foreign intelligence service. It reports to the Chief of Defence, but its remit covers both non-military and military issues. Its chief responsibilities are to alert to external threats to Norway and priority Norwegian interests, to support the Armed Forces and defence alliances which Norway is part of, and support political decision-making processes with information of special interest to Norwegian foreign, security and defence policies. FOCUS, its annual threat assessment, analyses the state of play and anticipated developments in thematic and geographical areas which the Service deems particularly relevant to Norwegian security and national interests.

THE DIRECTORATE FOR CIVIL PROTECTION is responsible for monitoring risk and vulnerability in society. Since 2011, the Directorate has assessed the risk of potential major incidents in Norway. They include natural disasters, major accidents or intentional acts. The risk analyses span different sectors and levels of public administration to capture knowledge and raise awareness of the broad range of ramifications and consequences. It has a longer time horizon than the annual assessments issued by the above-mentioned authorities.

FOREWORD

This open threat assessment considers a selection of crime threats. They have been selected based on their level of seriousness, and because the police consider the development to be negative. This is the first time after the police reform that the police prepare an open threat assessment, and we plan to do so every year.

The threat assessment is general in nature. The assessments are future-oriented, so as to inform planning and prioritising of measures to prevent and combat crime. All assessments about the future will necessarily involve a degree of uncertainty, so they are expressed using standardised probability terms.

The police are charged with counteracting crime and providing more safety and security for the public. The main strategy of policing, prevention saves economic and human costs. Prevention is better than cure. It is therefore important to the police to share knowledge of crime challenges with the public and our partners.

Prevention is not a task that can be solved by the police alone. Multiple parties have roles and responsibilities in preventative efforts. Parties other than the police will very often command the appropriate means and measures. Working together results in greater knowledge and more complete information on which to base measures which collectively have a preventative effect.

Benedicte Bjørnland
National Police Commissioner

CONTENTS

SUMMARY

New establishment, expansion of international criminal networks and recruitment of young people
It is likely that international criminal networks will seek to establish or expand their criminal activities in Norway. It is also likely that expansion and establishment will increase recruitment and tensions and lead to serious violent incidents. In case of expansion and new establishment, gangs need to recruit people to gang crime to bolster their position. It is highly likely that criminal groups will continue their recruitment of young people into gang crime, and that this will increase in connection with expansion and new establishment.

Potentially violent individuals with serious mental disorders
There are reports of an increase in incidents of people with serious mental disorders and problems with drugs or alcohol perpetrating serious violence and threats, and it is likely that the incidence of individuals committing acts of serious violence will rise. This is based on e.g. changes to the conditions for committal to psychiatric hospital.

Family members sexually abusing children, and domestic violence
Higher levels of unemployment and economic recession correlate strongly with increased risk of alcohol and drug abuse, anxiety disorders and depression. This may in turn lead to greater risk of physical or sexual abuse and neglect, both by people who are already abusive and people who have no such history. As a consequence, it is likely that some people will commit more physical and sexual abuse of family members. There is an even chance that children who have not previously suffered physical or sexual abuse by family members will become victims of such offences.

Network intrusion with ransomware
It is highly likely that there will be multiple successful network intrusions with ransomware against Norwegian enterprises. This is based on the steady rise in incidents in recent years and the potential for high profits. There is an even chance that enterprises with critical functions will suffer network intrusions.

Employers evading tax through undeclared labour
It is likely that there will be an increase in employers using undeclared labour. This is based on the greater demand for labour in sectors where tax crime and labour exploitation is rife. Growing sectors such as transport of goods and construction are particularly at risk.

Illegal fishing and under-reporting of catches in the fishing industry
Illegal fishing is camouflaged through under-reporting. There has been substantial and systematic under-reporting in parts of the industry for many years. It is assessed as highly likely that certain members of the industry will continue high-scale illegal fishing with under-reporting and misreporting of catches. This type of crime includes various forms of economic crime and employer crime. Illegal fishing is also environmental crime, as it undermines the sustainability of Norwegian fisheries management.

Misuse of identity documents by foreign nationals
Misuse of identity documents is a facilitator of various types of crime. The introduction of travel restrictions in connection with the coronavirus pandemic, with stricter border controls, fuels the need to enter Norway by fraudulent means. It is highly likely that a higher number of people will illegally enter Norway as so-called impostors, i.e. fraudulently using genuine identity documents issued to other people.

INTRODUCTION

The Police Threat Assessment (PTA) describes specially selected crime threats and gives a future-oriented analysis of them. Publication of the PTA is intended to promote a shared understanding of the crime challenges faced by society. It aims to provide a robust basis for working together to prevent and combat crime. The PTA will also support police decision-making in setting priorities and implementing effective measures for the whole range of police responsibilities. There are different parties preparing annual national threat assessments. The PTA covers a selection of serious crime threats that fall within the police's area of responsibility.

Commissioned by the National Police Directorate to support decision-making, the PTA has been prepared by the National Criminal Investigation Service (NCIS) in liaison with the police districts and specialist agencies. The Police Threat Assessment reflects the collective intelligence production of the police service. The report is also based on information from national and international sources, such as research reports and reports from various partners.

The police have a broad range of responsibilities, and crimes against individuals or society have different levels of seriousness. The crime threats highlighted in the PTA have been selected because they are deemed particularly serious. They have been assessed based on structured analytic techniques considering subjects' willingness and capability to commit crime, as well as the existence of a negative trend in the type of crime and the impact on individuals and society. The report has been prepared according to the principles of the Norwegian *Police Intelligence Doctrine.*

The descriptions of the crime threats have been aggregated and shortened in the report. Only the most relevant premises and causes are highlighted. The assessments have a perspective of up to one year. Unless otherwise specified, the assessments address the national level.

The report starts with a summary. It goes on to describe some of the most relevant factors that will impact how crime evolves. The report is structured around five main categories. Each starts with a brief definition of the category, for the purposes of this report. Then follow selected crime threats in each main category. After that, an assessment of anticipated developments for each threat and a description of the premises on which the assessment is based. However, some of the crime threats may fit into multiple categories. The assessments are in italics and placed in grey boxes. The threats are not presented in order of seriousness.

PROBABILITY TERMS

Any assessment will invariably be associated with some level of uncertainty. To handle this uncertainty in a standardised and coherent manner the report uses probability terms:

National standard	Description	NATO standard
Highly likely	There is very good reason to expect …	Highly likely (>90%)
Likely	There is reason to expect …	Likely (60-90%)
Even chance	There is an even chance ...	Even chance (40–60 %)
Unlikely	There is little reason to expect …	Unlikely (10–40 %)
Highly unlikely	There is very little reason to expect …	Highly unlikely (<10%)

FACTORS IMPACTING HOW CRIME EVOLVES

Norway has a general high degree of public order and security, and the public has a high level of confidence in the police and authorities in general. Crime in Norway is impacted by globalisation, digitalisation and technological developments.

However, the coronavirus pandemic and the associated measures to reduce infection rates impact daily life, work life and the economy. This leads to increased social insecurity and impacts crime.

The measures to reduce infection rates have accelerated digitalisation processes. This impacts the threat picture in digital space offering criminals more scope to operate, and the criminals are adapting to the situation. Travel restrictions impact cross-border crime, in particular by criminals developing new modus operandi for illegal entry and smuggling.

The current situation is also characterised by political movements and activism, protests and counter-protests, involving conflicts in public places. Gang conflicts will negatively impact public safety.

THREATS TO PUBLIC ORDER AND SAFETY

Threats to public order and safety means, for the purposes of this report, crime that reduces perceived safety in public places, such as conflicts and violent incidents. Below are selected, particularly serious crime threats in this main category.

New establishment and expansion of international criminal networks

It is likely that international criminal networks will seek to expand their activities in Norway. It is also likely that their expansion activities will involve increased recruitment, and that tensions will increase with serious violent incidents, some involving the use of weapons. The threat of violent confrontations can be heightened if the establishment challenges the interests of other criminal networks.

Criminal networks is an umbrella term covering circles, groups, gangs or sets of individuals united by crime. The criminal connections may be short-term or long-term in nature and involve all types of crime, and the networks may have a higher or lower degree of structure and organisation. The term thus covers everything from organised crime groups to criminal youth gangs. Gang crime is often considered to be a typical major-city phenomenon, but the gang term also includes 1% motorcycle clubs[1], and they are not limited to urban areas.

Several international criminal gangs have over time demonstrated their intention to expand their activities into or in Norway. Expansion activities tend to affect the existing balance of power between criminal networks and to be viewed as provocation, especially if the establishment takes place in the core area of already established networks. New establishment or expansion sometimes triggers serious acts of violence and/or major conflict. The serious acts of violence tend to involve knives etc. in public, though there are examples of guns being used. The acts of violence may negatively impact perceived local and general safety.

[1] 1% motorcycle club is the term used for motorcycle clubs that define themselves as outlaws living by their own laws outside Norwegian society. They consider themselves brotherhoods, with a large share of members having criminal records.

Recruitment of young people to gang crime

It is highly likely that criminal gangs will continue to recruit young people to gang crime. Recruitment strengthens the position of the gang, leads young people into a criminal lifestyle and negatively impacts perceived public safety.

Criminal gangs tend to be structured around a few leaders or an inner circle. The outer circle has runners whose gang affiliation is often loose. Runners are generally young people who are used for tasks such as drug dealing, hiding guns or committing acts of violence on behalf of the gang.

Even newly recruited runners are considered part of the criminal gang and enjoy its protection and a sense of belonging, but they can easily be replaced. Despite this, they play a key role in the commission of crime, so gangs rely on them for their business. Though constant, the need for recruitment increases in establishment or expansion phases and whenever the level of conflict becomes critical.

Gangs attract young people, frequently those of deprived or minority backgrounds, by offering a sense of belonging, brotherhood, respect, protection and financial means normally beyond their reach. Chain recruitment of entire groups of friends and through family members appears common. There are also examples of threats and force being used. There is targeted recruitment of young people with a capacity for violence and their own distribution networks for drug dealing. Much of the recruitment activity takes place on social media. They take and distribute images designed to brag about the lifestyle and music videos that glorify gangster life and show guns, money, celebrities and girls. Recruitment activities generally take place in the gangs' core areas and local communities of the young people.

Hateful and other criminal statements made in public

It is likely that the level of hate speech will continue to rise and have a polarising effect on Norwegian society. It is unlikely that the individuals making the statements will translate them into violence. However, as levels rise, hate speech may become normalised and inspire others, aggravating the potential for acts of violence motivated by hate.

In connection with protests to promote extremist views it is highly likely that individuals on both ends of the political spectrum have the capacity and willingness to commit serious acts of public disorder and of violence and provoke similar reactions in their opponents.

Freedom of speech has a strong position in Norway. However, some statements promote hate and are consequently criminal under Norwegian law. Hateful statements are racist or discriminatory, and some encourage physical violence. The Penal Code also protects people from discriminatory or hateful statements made in public (section 185). Some statements even incite violence. Rates of hate speech reported to the police have increased every year since 2015. The statements reported were chiefly motivated by ethnicity, but also religion, sexual orientation or disability.

The majority are made on social media, above all in Facebook groups or as comments left on various websites. The anonymity of users facilitates the phenomenon. Group dynamics lower many people's threshold for making ever more extreme statements. Negative comments also target politicians and other participants in the public discourse. Such statements may not constitute hate speech in a legal sense, but may still have implications for individuals, groups or society as a whole. So hate speech is a potential threat to democracy and negatively impacts the public discourse by discouraging people or groups from taking public office or participating in the public discourse due to the high cost involved.

Statements made in public, whether in digital space or not, are increasingly characterised by polarisation and extremism. Groups with extremist views and hostile messages organise protests with physical attendance that provoke a broad spectrum of the public. Coupled with extremist statements within or outside the boundaries of freedom of speech in digital channels, these may trigger acts of violence by opponents. Opponents have a variety of backgrounds and affiliations, include young people from minority groups and active members of far left-wing or right-wing political activist groups, as well as Islamist extremist.

THREATS TO LIFE OR HEALTH

Threats to someone's life or health means, for the purposes of this report, violence against or sexual abuse of children or adults. Violent crime can be physical, mental or latent[2] violence. Violence and sexual abuse takes place in the home, in public and online. Below are selected, particularly serious crime threats in this main category.

Potentially violent individuals with serious mental disorders

It is likely that more people suffering from serious mental disorders will commit serious acts of violence and constitute serious treats to themselves and others. Mental problems combined with drug or alcohol abuse, relationship problems or financial problems aggravate the risk of violence being committed.

Symptoms of, suspected or diagnosed mental illness in offenders are factors in a substantial share of reported homicides and attempted homicides since 2016, between 30 and 45 per cent. Nearly 60 per cent of offenders in these cases were considered *unfit to stand trial.* In 50 per cent of cases the offender acted under the influence of alcohol or drugs. Alcohol or drug abuse may aggravate the risk of violence in people with serious mental disorders.

The police and other partners are reporting an increase in cases of serious violence and threats perpetrated by people with serious mental disorders. Their victims may be random members of the public or people in their own close circle. The violence committed by persons with serious mental disorders is described as more severe and more ruthless than used to be the case. It includes threats with weapons in public places, e.g. replica firearms, knives, swords or axes.

The offenders are often well-known by mental institutions and the police. Although many of them are periodically detained in psychiatric wards, several will for extended periods of time not meet the conditions for committal, although their family and friends express concerns. The increases in cases of serious violence committed by individuals with serious mental disorders may be a consequence of the changes to the conditions for detention in a psychiatric institution in 2017. Persons with serious mental disorders who do not qualify for assistance from any support service or institution may be particularly aggressive or threatening in their behaviour. This may negatively impact public safety.

Domestic violence

It is likely that there will be an increase in domestic violence as a result of the coronavirus pandemic. This includes people with no previous history of violence and families with a history of violence.

[2] Latent violence is violence which is effective through its potential, i.e. the potential for violence will control the behaviour of the victim to avoid further violence (Isdal, 2000).

Every year both children and adults suffer violence at the hands of their closest family. This violence may be severe, in some cases lethal. Of all homicides committed between 2016 and 2019, 40 per cent of victims had a close relationship with the offender, i.e. they were partners, ex-partners, parents or children. Children are at particular risk of violence, both being subjected to and witnessing domestic violence. The offenders are generally men, both in terms of violence against children and against partners.

A 2020 report by the Norwegian Centre for Violence and Traumatic Stress Studies points out that there is a strong correlation between higher unemployment rates and economic recession, and heightened risk of alcohol and drug abuse, anxiety disorders and depression. This may in turn lead to greater risk of physical or sexual abuse and neglect, both by people who are already abusive and people who have no such history. Financial worries and loss of important social networks and support for the family may aggravate the situation further.

Family members sexually abusing children

There is an even chance that the rate of sexual abuse of children committed by family members will increase. Some children who have not been sexually abused before will become victims. This is based on the fact that family members have more opportunity to commit sexual abuse in the home due to the coronavirus pandemic.

There may be a variety of triggers of sexual abuse of children in the immediate family, including conflicts and crises caused by financial problems, alcohol or drug abuse, or mental illness.

Every year hundreds of children in Norway are sexually abused by a close family member. In 45 per cent of sexual assaults on children under 14 recorded in 2019, there was a family relationship between abuser and victim. The father or step-father was the abuser in the majority of cases, but many victims are abused by a brother, step-brother, grandfather or uncle. Abuse committed by a mother or step-mother tends to involve a man, as well. In many cases the offender abuses the victim over months or years, and the abuse may be severe. Multiple children in the same family may be abused by the offender.

Support organisations report an increase in children and young people who have experienced sexual abuse in their home contacting them since the implementation of the measures to reduce infection rates in March 2020. There is an increase in both calls about physical and sexual abuse, and incidents discussed are more serious than before the coronavirus pandemic. The abuse has happened during a period of time when the level of activities and services offered children and young people, as well as the capacity of social and health services, has been reduced. Many children have also stayed home more from daycare or school, giving abusers more opportunity.

Norwegian nationals ordering live-streamed sexual abuse

There is an even chance that a higher number of people with a sexual interest in children will order live-streamed sexual abuse, as travel to commit physical sexual abuse will be difficult in the coming year.

Europol has reported an increase in live-streamed sexual abuse of children by request in 2020. They see a connection with the fact that strict travel restrictions have prevented people who used to commit physical sexual abuse of children in other countries are now instead choosing to pay for live-streamed sexual abuse of children abroad. The Philippines report a substantial increase in such abuse during the pandemic, which can be explained through reduced opportunities for income in an already impoverished population, coupled with higher demand.

In recent years, several Norwegian nationals have been convicted of ordering live-streamed sexual abuse of children. Several of those convicted have been ordering abuse for many years, abuse which has been extremely serious in nature. Persons staying in Norway have mainly ordered live-streamed sexual abuse of children in the Philippines, but also of children in other countries, such as Romania and Madagascar.

The facilitators tend to be the children's carers who want to obtain money for the family. However, this type of crime may have a more organised character, with the money not going to the child's family, but pimps or other more professional facilitators. Payment for live-streamed child sexual abuse is principally made via payment transfer services and online payment solutions.

THREATS TO BUSINESSES AND IN DIGITAL SPACE

Threats to businesses and in digital space means, for the purposes of this report, crime committed over the internet. Cybercrime is mainly motivated by profit. Some cases of cybercrime are motivated by a desire to harm hardware or digital services or obtain sensitive information. The private sector, the public sector, critical services and private individuals are all targeted. Below are selected, particularly serious crime threats in this main category.

Network intrusion with ransomware

It is assessed as highly likely that Norwegian enterprises will experience network intrusion with ransomware. This is based on the steady rise in incidents in recent years and the potential for high profits. The identification of offenders and prosecution is extremely complex. There is an even chance that enterprises with critical functions will experience network intrusion.

Ransomware is the largest current cybercrime threat and has cost businesses hundreds of millions of NOK over the past two years. This is a type of malware used for encrypting files in the victim's computer system, before demanding ransom in exchange for recovery of the files. The method is complicated and requires sophisticated technical know-how. Recorded cases of ransomware, failed and successful attempts, have increased globally and in Norway since 2013. Globally there are an estimated 5 to 15 international attackers active at all times. In Norway we have reports that one attacker alone carried out more than 30 successful intrusions into the computer systems of Norwegian enterprises in the past year.

Ransomware and other types of cybercrime often start out in the same way, with the attacker making a wide search for points of access to the networks of potential victims. This may happen by way of social manipulation in emails (phishing), exploitation of software vulnerabilities, or password guessing (brute forcing). Once the attacker has obtained sensitive data, it may take several months for the ransomware to be activated, which makes it difficult to handle the incident immediately and trace relevant network activity. Although few network intrusion attempts are successful, there is a large potential for profit, and low chances of identifying and prosecuting offenders. Victims may suffer heavy losses. A known example is the 2019 intrusion into Norsk Hydro's computer systems, which cost the company about NOK 600 million.

The coronavirus pandemic has highlighted the vulnerabilities of public enterprises with critical emergency response functions. Internationally there are several reports of ransomware being deployed against national emergency response functions. Such an attack may ultimately lead to loss of lives or injury and harm public confidence in the compromised service.

Fraud targeting businesses

It is assessed as highly likely that criminals will increasingly target Norwegian businesses by way of invoice and CEO fraud. This is based on the potential for high profits, low risk of detection and the increase seen in recent years. Large companies are more vulnerable to targeted fraud attempts, and smaller companies to indiscriminate fraud attempts.

Criminals prefer two modus operandi: invoice and CEO frauds. In invoice fraud, the recipient of the invoice is deceived into paying for goods or services they never ordered, or the criminal will change the beneficiary bank account number on a genuine invoice by sending an email with "updated" payment details. In CEO fraud, the criminal obtains information about key individuals in an organisation. Pretending to be the CEO or another manager, the criminal contacts a financial officer of the organisation and instructs her or him to make a large payment to an account abroad.

Invoice and CEO fraud has increased in recent years. In 2019, CEO and invoice fraud constituted nearly 60 per cent of financial losses through deception in Norway. In 2019, 13 per cent of Norwegian enterprises reported that they had been victims of CEO fraud in the past year. Large enterprises are particularly vulnerable, but NGOs are also targeted. The substantial criminal profits are in many cases reinvested in other types of crime.

Invoice and CEO fraud by changing the beneficiary bank account number is perpetrated by organised crime groups abroad. The criminals appear adaptable; they carefully select targets and exploit human errors and/or vulnerabilities in computer systems. Financial losses through invoice fraud increased from NOK 8.7 million in 2018 to around NOK 138.5 million in 2019. Implications for individual businesses may be serious, and with its potential to drive businesses into insolvency, it may also have a serious impact on an individual level.

With many more people now working from home, businesses are even more vulnerable to invoice and CEO fraud. In 2020, Nordic Financial Cert saw an increase in CEO and invoice fraud. During the coronavirus pandemic, multiple invoice frauds related to infection prevention have been detected.

Investment fraud

The coronavirus pandemic has seen an increase in investment fraud, in particular shareholder fraud via bogus trading platforms. It is highly likely that investment fraud will continue to rise, both involving cryptocurrency and bogus trading platforms.

Investment fraud is deceiving private individuals or businesses into investing in projects or products that are worthless or non-existent. Social manipulation is a key part of the fraud process.

It is reported that investment fraud attempts doubled from 2019 to 2020. Several banks are reporting a rise in fraud attempts since 2018, with a spike in 2019 which continued in 2020. During the coronavirus pandemic many people, especially the elderly, have spent more time alone in their homes. This has made them more vulnerable to deception. A notable modus operandi of investment fraud is to offer for sale shares or cryptocurrency.

Ponzi schemes (pyramid schemes) involving the sale of cryptocurrency attract private individuals through promises of high returns. The expectations of value increase held out to investors are nothing but an illusion, because the cryptocurrency does not exist. The business model of a Ponzi scheme is to recruit new investors to secure more capital, which is paid to the fraudsters and lost by the investors. OneCoin is an example of such a Ponzi scheme. Organised crime groups in the

Balkans are believed to have obtained by deception around EUR 4 billion between 2014 and 2018 through this scheme.

Property fraud has proved lucrative in Norway. Fraudsters set up their own limited companies supposedly in property development, and deceive small savers into investing. They sell overpriced properties to the limited companies and keep the profit. One such example is the Indigo Finans case, where the company declared insolvency in 2017. The criminal case has been ongoing ever since and the estate in liquidation has around NOK 33 million in claims on it. However, investors and small savers are believed to have invested close to NOK 300 million in the company over several years.

THREATS TO SOCIAL STRUCTURES, FUNDING AND THE ENVIROMENT

Threats to social structures, funding and the environment means, for the purposes of this report, crime threatening Norwegian economy in the form of tax evasion or abuse of public financial support schemes. This threatens the funding of the Norwegian welfare state, distorts competition and is corrosive to public confidence in the systems designed to protect their rights and a fair labour market. The category also includes threats to the environment, such as illegal exploitation and trade in valuable natural resources, and savings made by breaching rules designed to protect against pollution hazardous to health and the environment. Environmental crime is often profit-motivated. Below are selected, particularly serious crime threats in this main category.

Employers evading tax through undeclared labour

It is assessed as likely that Norway will see an increase in employers using undeclared labour, based on the greater demand for labour in sectors where tax crime is rife. Growing sectors such as transport of goods and construction are particularly at risk.

Employers who systematically fail to report revenue and/or employ unrecorded workers are depriving the state of substantial income and driving those operating legally out of business. Furthermore, employees lose important welfare rights. Such businesses tend to employ illegal labour and to be largely cash-based. Undeclared labour may also involve laundering of proceeds from other types of crime.

The coronavirus pandemic has resulted in higher unemployment rates and a higher demand for services in sectors where tax evasion is rife. The authorities have uncovered organised fraud using fictitious employees to seek wage compensation for fictitious temporary lay-offs and camouflage undeclared labour. This allows criminals to save tax and fraudulently receive government compensation.

Undeclared labour is common in sectors using unskilled or low-skilled workers, such as construction and transport. Employers may operate individually or be part of networks with links to organised crime.

Illegal fishing and under-reporting of catches in the fishing industry

It is assessed as highly likely that some members of the industry will continue large-scale illegal fishing with under-reporting and misreporting of catches. It is assessed as highly likely that substantial illegal fishing of king crab will continue.

Fisheries crime means, for the purposes of this report, criminal offences that directly concern the value chains of the fishing industry. Illegal fishing and under-reporting and misreporting of catches are at the core of this type of crime.

A considerable problem globally, illegal fishing has contributed to the severe decimation of important commercial stocks, to the point of near-collapse. Although fish stocks in Norwegian waters are robust, fish, lobster and king crab caught wild are sought-after products with a considerable profit potential for the links in the production chain. Perpetrated by both Norwegian and foreign fishing businesses, illegal fishing constitutes a cross-border crime challenge. The fisheries sector is widely industrialised and integrated with the global market. This allows for sophisticated types of economic crime in Norway and abroad.

Illegal fishing is camouflaged through under-reporting. There has been substantial and systematic under-reporting in parts of the industry for many years. Vessels land fish that are not reported to the authorities, and are compensated through extra payment for the weighed, legal portion of the catch. Plants conceal under-reporting by overfilling boxes with fish or processing the fish themselves so as to change their weight. Invoices, landing and sales notes issued by plants indicate false quantities or species. This allows vessels' catches to be counted against quotas based on catches smaller than those actually landed. This MO lets vessels exceed annual vessel quotas and net high profits selling the extra catch. Plants get more raw material to sell for export.

In the king crab industry, some vessel owners charge a premium for the catches in return for landing large quantities of illegally caught king crab. The high prices commanded by king crab have led to large-scale illegal fishing. The crab is caught in Finnmark in the far north, while distribution networks operate throughout Norway.

Fisheries crime is a complex type of crime involving various forms of employer crime and economic crime. Illegal fishing is also environmental crime, as it undermines the sustainability of Norwegian fisheries management.

It has been uncovered that plants and fishing vessels are using irregular labour, exploiting foreign workers, partially undeclared. A common modus operandi is that workers must pay back wages and work in poor conditions. Fisheries crime entails substantial revenue losses for the Norwegian state.

Employers exploiting foreign workers

It is assessed as likely that Norway will see higher levels of, and more serious, exploitation of labour as a means to keep costs to a minimum and win tender contracts and contracts in general. It is also assessed as highly likely that some employers will continue to facilitate the entry of foreign workers in Norway. Often they will have to rely on misuse of identity documents. In addition, it is highly likely that there will be a will rise number of foreign nationals using false employment contracts to qualify for entry into Norway on false grounds. This is the result of measures implemented in connection with the coronavirus pandemic.

Employer crime[3] takes place in sectors with a high proportion of unskilled workers, lack of regulation, low establishment costs and extensive use of sub-contractors. They include agriculture,

[3] Employer crime involves breaches of Norwegian rules and regulations on pay and working conditions, national security contributions and taxes, frequently perpetrated in an organised manner exploiting workers or distorting competition, and having a corrosive effect on social structures. It tends to be accompanied by other types of crime.

fisheries, transport and construction. Employer crime takes place throughout Norway, with perpetrators ranging from small business owners to networks affiliated with serious organised crime. The coronavirus pandemic has sharpened competition in a number of sectors.

Some employers in sectors using unskilled or low-skilled workers recruit foreign workers to minimise pay costs and costs associated with mandatory health and safety measures. Workers are not paid their due wages and are not entitled to sick pay or similar benefits. Misuse of identity documents is a key part of employer crime. Stating a false identity, a third-country national can give the appearance of being an EEA-citizen entitled to work in Norway. This lets foreign nationals enter Norway on false grounds and gain rights to which they are not entitled.

Foreign nationals without legal residence or valid work permits are intimidated into accepting lower than legal pay and unacceptable working conditions out of fear of being deported. Employers are both Norwegians and foreigners. The exploitation is often concealed in a chain of sub-contractors, or by encouraging the foreign national to work for one-man businesses with fewer welfare rights. Employers complying with the law risk being driven out of business by competitors operating illegally.

The recruitment of foreign labour has become lucrative. Recruiters tend to recruit fellow countrymen. 2020 saw numerous cases of people presenting false employment contracts at the border to circumvent travel restrictions imposed due to the coronavirus pandemic. On social media and in foreign newspapers recruiters advertise the sale of "employment contracts" in Western Europe and Norway.

Business owners committing insolvency crime

It is likely that insolvency crime will rise and be camouflaged in the mass of insolvencies resulting from the financial struggles of the coronavirus pandemic. Business owners will seek to illegally maximise profits from businesses that are no longer viable before declaring insolvency.

The great majority of insolvencies do not involve criminal offences. However, there has historically always been widespread insolvency crime in the wake of financial crises. A higher level of insolvencies makes in more difficult to detect this type of crime.

In insolvency crime, companies are illegally drained of funds while still trading. Assets may be sold off cheaply, or funds moved to other businesses. Ahead of insolvencies there is often fraud on credit institutions and investors by wrongfully injecting operating capital into no longer viable businesses. Insolvency is also used as a means to commit or conceal other financial crime. Insolvency crime imposes high financial losses on creditors. Furthermore, this type of crime may distort competition and harm individuals, who never receive the goods or services they have paid for.

Both individuals and organised criminals commit insolvency crime. They tend to operate with multiple companies, regularly changing the addresses and names of businesses. Though banned from running businesses, many offenders go on registering businesses in other people's names to avoid detection. A 2019 review of criminal employers found that 45 per cent were registered as holders of leading roles in businesses that failed.

2020 has seen fewer compulsory liquidations and insolvencies than the two previous years. Part of the reason is that businesses have, throughout 2020, been given extensions to due tax payment dates and compensation though various government support schemes. Several businesses have low liquidity due to the coronavirus pandemic, particularly following the second lockdown in the autumn

of 2020. These will have problems paying outstanding taxes in addition to those triggered by taxable coronavirus financial support. Due dates were extended to spring 2021.

THREATS TO BORDER AND INTERNAL SECURITY

Threats to border and internal security means, for the purposes of this report, crime threatening internal and external Schengen zone borders and territorial security. This includes misuse of identity documents and cross-border crime such as smuggling of goods or migrants, as well as illegal entry and stay. Below are selected, particularly serious crime threats in this main category.

Misuse of identity documents by foreign nationals

It is assessed as highly likely that Norway will see an increase in imposters[4] misusing genuine documents for illegal entry. The introduction of travel restrictions during the coronavirus pandemic, with stricter border controls, fuels the need to enter Norway by fraudulent means. The emergence of other types of identity fraud such as morphing[5] challenges detection further. There is deemed to be an even chance that this modus operandi will be used for illegal entry into Norway.

Two types of misuse of identity documents that represent particular threats to public security are imposture and morphing. Both types can be hard to detect, and so attractive modus operandi to criminals. Frontex has over several years assessed imposture as the greatest ID fraud threat in Europe. Norwegian authorities have detected few imposters, though more often in recent years.

Morphing is an emerging threat which Frontex refers to as a global security threat. The MO circumvents biometrics systems at borders and is extremely difficult to detect by regular inspecting officers. It is easier to morph images than counterfeit a document. No cases of morphing have been detected in Norway as yet, but cases were detected elsewhere in Europe in 2020.

There is an increasing offer of false and genuine identity documents, including Norwegian passports, being traded openly on digital platforms. Documents from EU and Schengen-zone countries are especially attractive, as their users are subject to fewer checks. The demand for and offer of identity documents is considerable, with sellers seldom facing prosecution.

Misuse of identity documents is a facilitator of various types of crime, including people smuggling, human trafficking and employer crime. Stricter border controls have fuelled such fraud. It represents a threat in that the true identities of foreign nationals entering and staying in Norway remain unknown. They may gain rights to which they are not entitled, such as social security benefits or Norwegian citizenship on false grounds. Furthermore, they may commit repeated and serious crime and be expelled from Norway, but cannot be deported back to their home countries because their identities are unknown. Persons using false identities may also perform work subject to licensing for which they are not qualified.

[4] *Imposter* – a person pretending to be someone else by using a genuine identity document issued to that person.
[5] *Morphing* – a technique morphing two or more photos and manipulating them to resemble both pictured individuals.