



ØKOKRIM

2022

# Threat assessment





## Probability levels

Any assessment will invariably be associated with some level of uncertainty. We therefore use probability levels to denote how confident we are in our assessment. The probability levels are standardised and are the same as those used by the Police Security Service, the Armed Forces and the police in general. The probability levels are highlighted in italics.

**Highly likely:** There is very good reason to expect ... More than 90% probability

**Likely:** There is reason to expect ... 60–90% probability

**Even chance:** There is an even chance ... 40–60 % probability

**Unlikely:** There is little reason to expect ... 10–40 % probability

**Highly unlikely:** There is very little reason to expect ... Less than 10% probability

# Preface

In this report we present what Økokrim believes will be the biggest threats within our area of responsibility in the coming years. We present a current picture of the crime situation in Norway and expected trends. The threat assessment is built on Økokrim's and the police's total intelligence output. Also, the report is based on information from national and international sources, e.g. scientific research and reports from various partners.

Økokrim published its last threat assessment in 2020, at the start of the Corona pandemic. Some of the threats we identified related to the effect of the pandemic on crime have materialised while others have not, or only to a lesser degree. We hope that the reason some of the threats we identified did not materialise is that society managed to implement risk-reducing measures because we identified them as threats.

The crisis we as a society have faced over the last two years has been managed, although some of the effects will be long-lasting. At the time of the publication of this threat assessment we face a new crisis created by Russia's invasion of Ukraine. The war in Europe is already having noticeable effects on crime in Norway and will continue to do so. We have taken the effects of the war into account in this assessment, both by pointing to the threat of exploitation of Ukrainians in the labour market and the threat war and polarisation poses to other financial and environmental crime.

The effect threat assessments have is

difficult to measure, but the main reason for publishing assessments of the threats within our area of responsibility is to enable both public and private sector actors to find and implement appropriate measures to counter financial and environmental crime. We hope that individuals and organisations who read this report will use it in their efforts to reduce the risk of financial and environmental crime, and we hope it will be of use to the Norwegian public, which needs information to assess expected developments of financial and environmental crime.

Threat assessments are not made in a vacuum. I would like to thank all our partners who have contributed the information on which this threat assessment is built.



Pål K. Lønseth  
*Head of Økokrim*

---

Threat assessment 2022, Økokrim

Photo: iStock, Shutterstock and Unsplash

Graphic design: Økokrim.



# Highlights



## War and polarisation, pages 6–15

- The war in Ukraine will effect crime in Norway.
- Exploitation of foreign workers occurs particularly in labour-intensive industries. It is *likely* that criminal actors will try to exploit Ukrainians and other foreign and vulnerable workers.
- It is *highly likely* that romance scams will continue to be a problem. It is also *likely* that the war in Ukraine will be used to provide cover stories for scammers aiming to defraud people.



## Sustainability, pages 16–37

- One of the greatest challenges for Norway in achieving the UN's sustainability targets is our high material consumption. The high cost of environmentally friendly waste management and recycling combined with the high cost of some components make it *highly likely* that both Norwegian and foreign actors can profit from illegal waste management and sale of discarded products.
- It is *likely* that both private individuals and commercial companies will commit large-scale, illegal destruction of nature through deforestation, digging, blasting, landfilling and depositing of waste.
- A large part of the financing of the welfare state comes from taxes and duties on income, expenditure and wealth. Fisheries crime, tax fraud and exploitation of workers threaten these tax bases. It is *highly likely* that some actors systematically underreport their fish and shellfish catches. It is also *highly likely* that many actors in various industries will continue to underreport or fail to report wages and turnover.
- It is *likely* that the risk of corruption in the local government level is at its highest in connection with tender processes. Our investigations indicate that corrupt practices can continue undiscovered for many years.
- It is *likely* that maltreatment of animals will increase due to the many pets acquired during the pandemic. Digitalisation has also eased contact between people who want to maltreat or have sex with animals.



### **Virtualisation, pages 38–49**

- We expect that criminal networks increasingly will adopt new technological solutions to commit financial crime in the years to come. It is *highly likely* that there will be increased use of deepfake in CEO frauds.
- Online and computer fraud is the new burglary and the crime people are most likely to become victims of. It is *likely* that fraud attempts will be automated and increasingly adapted to the individual recipient.
- It is *likely* that virtual assets increasingly will be used to launder money. This because virtual assets is becoming ever more common within finance, art and online gaming.
- Money mules are used particularly in connection with online and computer crime. It is *likely* that there will be an increase in the use of money mules in the years to come.



### **Glocalisation, pages 50–66**

- National borders have become less important, and crime committed in one country may have local consequences elsewhere. Digitalisation and integration of national economies and labour markets are drivers in cross-border crime.
- Government financing schemes and tenders to promote the shift to a green economy will *highly likely* be exploited by Norwegian and foreign actors.
- It is *likely* that increased competition for resources and limited transport capacity will increase the risk of Norwegian companies paying bribes abroad.
- Criminal networks influence decisions in some companies and professional actors and straw men are used to conceal criminal acts and corporate ownership. Some industries are now characterised by tax fraud, exploitation of workers and poly-criminality.

# War and polarisation

World events are currently marked by the war in Ukraine and increased polarisation between East and West. After years of increased democratisation and western orientation by countries in Eastern Europe, Russia has gradually escalated its use of force against several previous Soviet Republics. The war in Ukraine will have dramatic consequences for Europe and lead to permanent changes in the world order. The war has also caused large numbers of Ukrainians to flee to other European countries. Also, the tense security situation in the world has drawn attention to hybrid threats.

The war in Ukraine has led to increased unity in both NATO and the EU after several years marked by Brexit.

The sanctions against Russia and Russian nationals demonstrate how the means of exercising power and the channels through which it is exercised are changing, and how the sanctions have large consequences far beyond the directly involved countries and individuals.

The sanctions against Russia also bring up the challenges posed by jurisdictions of secrecy – so-called tax havens – which are countries with low taxes, few regulations and little openness about ownership of companies and bank accounts.

The war also has consequences for the

supply of food and energy in many countries on several continents. Russia and Ukraine alone account for around one-third of all wheat exports, but the war will make it difficult for the two countries to maintain their farm production and wheat exports. This may lead to increased risk of smuggling of food and other goods. We also expect commodity prices to increase following reduced Russian export of for example steel and iron. The demand for Russian gas is also a challenge for Europe. A limited supply and the ensuing higher prices may lead to social and political unrest in other parts of the world. The risk of corruption is also expected to increase.

Russia's invasion of Ukraine also increases the risk of radiation as a result of nuclear



incidents and the risk of radioactive and nuclear substances being lost or falling into the wrong hands. Radioactive waste does not respect national borders and can be spread over large areas depending on the force and direction of the wind. The consequences for Europe – including Norway – of a nuclear incident may be very serious.

The Arctic is where Norway has its most important strategic interests. An ice-free Northeast Passage may shorten the trade route between Europe and China and lead to increased traffic in the area. Also, China will continue to prioritise its long-term position in the Arctic, e.g. for future extraction of resources.<sup>1</sup> At the same time, civilian and military activity in the Arctic and its strategic importance and role are expected to increase as a result of growing

superpower rivalry.

Offshore investments in the Norwegian sector of the Barents sea and maintaining the Norwegian population and Norwegian ownership of infrastructure and control of the natural resources on Svalbard will be important in the years to come. Norway's relationship with Russia will also remain important.<sup>2</sup>

Use of social media has democratised the production of information. Many more people produce information, and young adults increasingly avail themselves of other sources than quality-assured information from mainstream media. In the USA, fake news and information campaigns have been used to increase the polarisation of society. Fake news and disinformation are also used actively in the war in Ukraine.

<sup>1</sup> PSS, "National threat assessment 2021" 2021.

<sup>2</sup> Ministry of Defence, "Parliamentary bill 14 S (2020-2021). Defensive and emergency response capacity. Long-term plan for the defence sector", 2020.



# The war affects crime

The war, its direct consequences and the consequences of the sanctions imposed by the West have already had effect on crime in Europe.

Ukrainian and Russian criminal networks have used ports in Ukraine as entry points for smuggling both people and goods into Europe. These networks are expected to reorganise their activities, exploit new opportunities and strengthen their position as a result of the war. They may also move their criminal activities to other countries.

War increases the risk of destruction and plundering of and illegal trafficking in art and cultural heritage objects. There are seven UNESCO world heritage sites in Ukraine. It is uncertain whether they have been affected by the war, but objects have disappeared from one museum in the country.<sup>3</sup>

Ukraine is both a source of and a transit country for trafficking of plants and animals to Western Europe, and the country is believed to be the largest exporter of illegal timber to the EU. This activity will probably resume and may increase in the wake of the war.

Several million people have fled Ukraine, and

the refugees may include members of criminal networks. The biggest threat in connection with the refugee situation is, however, people smugglers and other actors who try to exploit vulnerable refugees for prostitution or forced labour.

A number of fundraising initiatives have been launched on social media in support of Ukraine's war effort and for humanitarian aid. Not all of these are honourable. War appeals to people's feelings, and this will probably be exploited by fraudsters.

The war in Ukraine also brings to front the use of hybrid threats.<sup>4</sup> There has been a rise in cyberattacks in recent years, and criminal networks in Ukraine and Russia are known for their involvement in cybercrime.

Russia's import restrictions and the sanctions imposed against the country also highlights the smuggling of fish from Norway via third countries.<sup>5</sup>

<sup>3</sup> The Guardian, "Cultural catastrophe: Ukrainians fear for art and monuments amid onslaught", 2022.

<sup>4</sup> Combined threats are known as hybrid threats.

<sup>5</sup> IntraFish.no, "Korrupsjonsekspert mener Vietnam-eksportører kan straffes", 2018.



## Exploitation of vulnerable workers

Exploitation of foreign workers takes many forms and has different underlying causes. It is *likely* that criminal actors will try to exploit Ukrainians and other foreign and vulnerable workers for undeclared and illegal work.

Refugees and foreign workers are particularly vulnerable due to poverty and lack of language skills and education. Exploitation is common particularly in labour-intensive industries with a large proportion of unskilled workers, e.g. construction, car valeting and repair, goods transport, cleaning and seasonal work within agriculture and fishery.

The use of illegal labour has for many years been widespread. In some cases, employees who work illegally are also exploited. The use of illegal labour increased at the end of 2021 and persists in 2022 after having seen a dip during the Corona pandemic.

Already before the Russian invasion, Ukrainian nationals were being exploited for illegal work in various industries in Norway, e.g. construction and seasonal work in agriculture. In these industries, plus cleaning and waitering, there is a high risk that Ukrainian refugees will be exploited. Both Ukrainian women and underage children have reportedly been offered illegal work in Norway before they were granted collective protection. Some were offered work before they arrived in Norway, while others

have been approached by recruiters in Norway. Collective protection grants Ukrainian nationals temporary residence and work permits in Norway. This may reduce their vulnerability in the labour market.

Increased demand for goods transport has made the large transport companies dependent on contractors. The use of contractors makes it hard to monitor the drivers' working conditions. Many contractors and sole traders in the goods transport industry do not declare their drivers' pay and subject them to poor working conditions and low wages.<sup>6</sup>

Employers unlawfully enriching themselves on their workers' wages and other remuneration is also a form of exploitation. Foreigners who work without being recorded in the employee register and who receive their wages in cash, make it harder for the authorities to uncover these practices. This gives criminal actors more opportunities and make foreign workers more susceptible to exploitation.

<sup>6</sup> Økokrim, "Kriminelle aktører i varetransportbransjen", 2022.



Some drivers in the goods transport industry experience heavy pressure and work so long hours that they don't have time to go to the toilet and instead urinate in bottles in the lorry.



## Norway as transit country for illegal funds

One way for foreign criminals to legitimise the movement of funds is to use Norwegian financial institutions to make transfers. Norwegian banks are *highly likely* being used to channel funds by both foreign individuals and companies who wish to mask both the origins and recipients of money laundering and other criminal transactions.

Norway is considered a low risk country and transfers via Norwegian banks or companies give the funds a semblance of legitimacy. Many tens of thousands of bank accounts in Norway are held by foreign companies and are used to make transactions of large amounts which are relatively quickly channelled to accounts abroad. Making transactions through shell companies located in tax havens further conceals the origin of the funds.

The leaked FinCEN files revealed that as much as NOK1 billion may have been channelled through various accounts held with the Norwegian bank DNB. Suspicions are that the funds can be linked to money laundering, corruption and financing of terrorism.<sup>7</sup> Also, the transfers suspected of being bribes made by the Icelandic company Samherji to key

politicians and civil servants in Namibia, show how Norwegian banks can be used as a transit country for moving money.<sup>8</sup>

Bank accounts held by private individuals are also used to move funds. The holders are often of foreign origin and the funds are often received from countries in Asia, and in a few years they can transfer many million NOK.

It is hard for Norwegian banks to clarify customer relationships, ultimate beneficiary owner, sender and recipient when shell companies, tax havens and client accounts are used to make a transaction.

Following the Russian invasion of Ukraine, western countries have introduced a number of sanctions and restrictions on Russian and Belorussian nationals, companies and interests. As a result there is a risk that Russian and Belorussian actors will try to transfer assets via Norway.<sup>9</sup>

<sup>7</sup> Aftenposten, "Derfor er dokumentlekkasjen FinCEN Files viktig", 2020.

<sup>8</sup> Dagens Næringsliv, "Islandsk nettsted: Samherji skal ha brukt DNB for å sluse penger via skatteparadis", 2020.

<sup>9</sup> Dagens Næringsliv, "Jurist Julie Odden: - Veldig sannsynlig at sanksjonerte russere nå prøver å bruke Norge til å sluse penger videre til andre land", 2022.



## Hybrid threats - Ownership and control of Norwegian enterprises, real estate and investments

Hybrid threats can be understood as government and non-government actors' threat or use of a combination of measures to exploit vulnerabilities, foment unrest and achieve certain political or strategic aims.<sup>10</sup> It is *likely* that foreign states will attempt to invest in Norwegian real estate, securities, business and industry in order to gain influence and access to information contrary to Norwegian interests.

Norwegian companies offer goods, services, technology and competencies which are important to other states. This may motivate foreign take-overs and investments.<sup>11</sup> Investments can increase a foreign state's ability to infiltrate, surveil, spy on and sabotage goods, services and functions critical to our society, economy and military defence.<sup>12</sup>

Whether foreign ownership can constitute a threat depends on a number of factors, e.g. ownership share, business concentration in the sector and the cost of switching to a new supplier. Another important factor is the access the ownership gives to technology and

resources. There are, for example, many oil companies, but only a few possess technology of interest to foreign powers. In the Bergen Engines case in 2021, these were among the factors which were decisive in the Norwegian government's decision to stop its sale to a Russian company.

Companies that operate infrastructure critical to society are also companies where foreign ownership may constitute a threat to Norwegian interests.<sup>13</sup> Foreign investment funds can buy up sufficient securities to obtain control over and influence in a company. They can do this to gain access to technology and competencies, influence decision makers or sabotage the company to diminish the host country's capabilities. Investments by foreign companies can be made on behalf of foreign governments and have ulterior motives other than financial gain.

<sup>10</sup> Phillips, Aleksander & Austad, Håkon, "Politiets rolle i deteksjon av sammensatte trusler", Masteroppgave PHS, 2017.

<sup>11</sup> PST, "Nasjonal trusselvurdering 2022", 2022.

<sup>12</sup> NUPI, "Hvorfor investerer Kina og Russland i Norge", 2021.

<sup>13</sup> FFI, "Utenlandske investeringer og andre økonomiske virkemidler – Når truer de nasjonal sikkerhet?", 2021.





## War as deception ploy in romance scams

Romance scams are a type of fraud that exploit people's desire to be loved and to help and care for others. In this type of scam, the perpetrators cultivate a relationship with the victim over time before the fraud is committed. By devoting ample time to build a relationship, the perpetrator builds greater trust, something which is then often reflected in the amount the victim is defrauded of. The perpetrators are cynical professionals. It is *highly likely* that romance scams will continue to be a problem. It is also *likely* that the war in Ukraine will be exploited by scammers as a cover story to defraud victims.

Contact with victims is often established on dating sites and various applications, but also on gaming platforms and on social media. The perpetrators create fake profiles and use photos stolen from real persons, often posing as military personnel, doctors or aid workers. The cover story is that they are deployed in a war zone. Both Afghanistan and Syria have been used for this purpose, and we expect that the war in Ukraine will be used in the same manner.

Through social media and regular contact via private channels, a story is established to induce the victim to send money. Gradually, the

"boy/girlfriend" starts experiencing problems and needs money to pay their way out of them. The amounts are often small at the start and then increase gradually. A new trend is that the perpetrator claims to have sent a valuable gift and then asks the victim to pay customs or other duty or charge. The fraud often goes on for several years and the victims lose large amounts of money.

In cases where the bank suspects fraud, they contact the victim, but it is often hard to convince victims that they have been manipulated, as they are caught in an emotional relationship they find it hard to break out of.

Victims are generally women aged 50–80<sup>14</sup> who have created profiles on social media or dating sites. In many cases, the victims are also used as money mules.<sup>15</sup>

<sup>14</sup> DNB v/FC3, "Annual fraud report 2021", 2022.

<sup>15</sup> Money mules are people who receive money from one person and then transfer them to another, either digitally or in cash, commonly against payment.

# Sustainability

Sustainable development meets both the needs of the current population and the needs of coming generations. Sustainability is about protecting the fundament of life – the earth itself – i.e. the climate, environment and biodiversity. A sustainable economy requires developing an economy that can provide all people with good living conditions, including access to good health care, education, a decent job, equality between the sexes and cultural diversity.

The UN's 17 sustainability goals are divided into three dimensions – economic, social and environmental. Norway has committed itself to work to achieve the goals within 2030. The biggest challenges facing Norway are linked to our high material consumption and large emissions of climate gases per inhabitant. Norway is number six of 169 countries with respect to consumption of material resources per capita, and one of the 30 largest emitters of CO2 (not counting absorption of CO2 in forests).<sup>16</sup>

Climate changes will have considerable negative impact on nature and people's lives and health. The short-term consequences include loss of life, heightened socioeconomic and geopolitical tension and negative economic effects. Climate-related natural disasters like

hurricanes, drought and large wildfires have already become more intense and frequent. The polar ice cap is melting at a faster pace and heatwaves have become more common.<sup>17</sup> Norway can expect a warmer and wetter climate with more intense precipitation, larger and more frequent floods, rising sea levels and more landslides.<sup>18</sup>

The diversity of plants and animal species necessary to sustain ecological systems and processes is threatened by climate change and overexploitation of nature. Loss of biodiversity is considered one of the main threats facing humanity today. Humans have already killed 83 per cent of all wild animals and destroyed half of all wild vegetation.<sup>19</sup>

Climate change is also expected to lead to

<sup>16</sup> Kommunal og moderniseringsdepartementet, "Meld. St. 40 (2020 –2021). Mål med mening. Norges handlingsplan for å nå bærekraftsmålene innen 2030", 2021.

<sup>17</sup> World Economic Forum, "The Global Risk Report", 2020.

<sup>18</sup> Aamaas, Borgar; Aaheim, Asbjørn; Alnes, Kristina; Oort, Bob van; Dannevig, Halvor & Hønsi, Torun, «Oppdatering av kunnskap om konsekvenser av klimaendringer i Norge», CICERO Center for International Climate Research og Vestlandsforskning, Report 2018:14.

<sup>19</sup> World Economic Forum, "The Global Risk Report", 2020.



increased migration, and scarcity of resources may trigger conflicts and wars. This may hamper the world economy, lead to unstable food prices, supply line disruptions, changed production and trading patterns, and fluctuations in the value of Norway's sovereign wealth fund.<sup>20</sup>

The melting of the Arctic ice cap opens a new northern sailing route. More ships sailing along the Norwegian coast will entail risk of serious pollution in a vulnerable area far from established emergency response structures. Higher temperatures also lead to many species of fish migrating north from tropical areas.<sup>21</sup> Warmer water and less ice in the Barents Sea also leads to a longer fishing season in an already vulnerable marine ecosystem.<sup>22</sup>

Sustainability is also about good management of the economy. The Norwegian welfare state is mostly financed through the payment of taxes, customs and excise duties, and the production of goods and services.

The current global business model which focuses on lowest possible production costs

and value chains, leads to income being channelled to countries where taxes are lowest, also known as tax havens. It has been estimated that tax planning by large multinational companies and rich individuals leads to the evasion of USD 483 billion from taxation annually. The evaded taxes are funds which could have benefitted the population in general, e.g. in the form of better welfare services.<sup>23</sup>

The tax base will also come under pressure from higher expectations of reduced emissions of climate gasses. The shift to a green economy will require investments in renewable energies. Higher commodity prices will also make the shift more costly.

Norway has a strong welfare state. Small social differences and political stability help suppress polarising and populist tendencies and reduced trust in government authorities. Nevertheless, the need to make unpopular decisions with a wide impact on people's daily lives, may challenge political stability in Norway. So can high electricity prices.

<sup>20</sup> NOU, "Klimarisiko og norsk økonomi", 2018.

<sup>21</sup> Havforskningsinstituttet, "Klimaendringene i havet skjer, vi må handle nå", 2022.

<sup>22</sup> Havforskningsinstituttet, "Flere følger fisken nordover når isen smelter", 2020.

<sup>23</sup> Tax Justice Network, "The State of Tax Justice 2021", 2021.



# Climate and nature crime

The legal protection of the climate and natural environment is often violated when it clashes with the demands of infrastructure construction, local government autonomy and economic growth. The UN Secretary-General calls this "a criminal denial of responsibility". The climate crisis and increased focus on the environment is changing our perception of what constitutes serious crime.

The consequences of the interaction between climate change and destruction of nature is gaining increasing emphasis. The term "climate crime" equates actions that lead to greenhouse gas emissions and global warming with crime.<sup>24</sup>

In Norway and abroad, environmental organisations initiate legal action against companies and governments, demanding reduction of emissions and compensation for climate damage. Many countries in Europe are demanding a dedicated environmental crime prosecutor at Eurojust and the adoption of international legislation to combat the most serious environmental crime.

Serious climate and nature crime is committed by both companies and individuals. Companies commit serious pollution crime, e.g. by violating discharge permits as a result of lacking maintenance, accidents or the desire for increased profits.

In the global fisheries industry it is estimated

that 10 per cent of catches are thrown back into the sea.<sup>25</sup> That large quantities of fish are thrown back into the sea has been uncovered also in Norwegian waters. These quantities are neither recorded nor used as a resource.

Another persistent threat is illegal hunting, particularly of wolves. There are suspicions that wolves are driven from their territories so that they can be hunted "legally" outside the protected wolf zone.

Motorised traffic in nature is prohibited, with some exceptions, e.g. necessary transport of goods or on designated paths. Illegal traffic outside inhabited areas with snowmobiles and other terrain-going vehicles is on the increase in many police districts. This activity is a threat to nature and wildlife and pollutes through noise, smell and exhaust emissions. The risk to life and health is substantial, and driving under the influence of alcohol and other intoxicating substances is widespread.

<sup>24</sup> White, R. Climate change criminology, Policy Press, 2018.

<sup>25</sup> Havforskningsinstituttet, "Estimering av utkast i norsk kystfiske med garn", 2021.



## Crime related to the circular economy

Circular economy and recycling of waste are increasingly important in many industries, e.g. petroleum, shipping, fisheries, aquaculture and construction industries. Businesses in these industries have an incentive to dispose of discarded vessels, installations and buildings in the cheapest way possible. There is an *even chance* that some Norwegian actors will try to violate laws and regulations to reduce costs.

The climate goals set in the Paris agreement force Norway to reduce its petroleum industry. Several of the facilities on the Norwegian Continental Shelf have reached a mature phase, and 278 wells on the Shelf will cease production over the next ten years.<sup>26</sup>

A number of yards in Norway specialise in removal of offshore installations, and the market is expected to grow. Strict environmental and HES regulations apply, but one company has been reported to the police in 2022 for careless handling of explosives and illegal blasting outside when breaking up an obsolete oil installation. There are also many laid-up offshore vessels anchored along the Norwegian coast. If businesses chose cheap rather than environmentally friendly solutions, the decommissioning of retired oil installations and offshore vessels may become a substantial environmental hazard.

Breaking up discarded ships is basically an

environmentally friendly industry that contributes to sustainable development by recycling iron and other materials. The number of ships being scrapped has increased in recent years due to the phasing-out of single hull ships.

The challenge is that of 763 ships discarded in 2021, 583 ended up on beaches in Bangladesh, India and Pakistan. The number of ships with Norwegian owners ending up here has reportedly increased since 2015.<sup>27</sup> Supertankers, car ferries and container ships are beached at high tide and then broken up at low tide. The ships are cut up manually on the beach under hazardous working conditions. Dangerous waste and chemicals are dumped or released into the immediate environment and cause serious local pollution.

Ships sailing in Norwegian waters cannot legally be sent for scrapping on the Indian subcontinent. The use of intermediaries when selling ships is common, however, and this makes this type of crime hard to uncover and prosecute. In 2020, a Norwegian shipping company was convicted of illegally having tried to export a ship for scrapping. The ship was on its way to Gadani, Pakistan, when the engines failed and the ship came adrift off the Norwegian coast. This is the first time that Norway has stopped, taken arrest in a ship and prosecuted a shipping company for this type of crime.

<sup>26</sup> Offshore Energies UK (OEUK), "Decommissioning insight 2021", 2021.

<sup>27</sup> NGO Shipbreaking platform, "2021 Annual list of ships scrapped worldwide", 2022.





## The waste management market attracts criminals

Pollution as a result of illegal waste management constitutes a serious environmental threat. Waste management crime may involve theft or illegal dumping, storage and export of waste. Both private persons and companies are involved. A continued increase in the consumption of goods will result in more waste. The combination of higher prices on waste and higher cost of waste management makes it *highly likely* that foreign and national criminals will commit waste management crime.

A circular economy means that a product's life is extended. At the same time, waste is already in high demand and components can be traded at high prices.

The waste management industry has a so-called "reversed" economy in which the income is generated on the receipt of waste while the expenses are incurred when it is responsibly disposed of, and the cost of legal waste management is expected to rise. Waste is often exported to countries where environmental standards are less demanding, particularly for the handling of paper, plastic and metals.

The waste management industry has a particularly high risk of environmental crime, also in Norway. Inspections have demonstrated that many waste disposal plants do not comply with permissions and store waste in ways that risk pollution or fires. A waste disposal company was in 2022 fined NOK1.5 million after large quantities of tyre scraps were found on

the seabed outside the plant. In 2019, 30 tons of tyre scraps were removed from the area. Another waste disposal company is under investigation suspected of multiple violations of the Pollution Control Act. Illegal waste management may also involve reintroducing waste into the product cycle, the sale of hazardous waste that is then mixed with other waste, or the reuse of waste.

Theft of e-waste from collection points is a problem in many Norwegian cities despite many dealers having put locks on their containers. Dealers of electric and electronic goods experience that their locks are forced open, surveillance cameras disabled and their staff threatened. In and around Oslo theft and illegal export of e-waste is committed by both locals and itinerant workers. GPS tracking of e-waste and selected vehicles has shown that Norwegian waste ends up in Nigeria, Romania and Lithuania. Catalysers are stolen from parked vehicles, car breaker's yards and recycling companies, and exported illegally.

Illegal waste export may have serious consequences for both humans and nature in the countries to where it is exported. Theft and illegal export of discarded electric and electronic goods generate profits for criminals and substantial losses for Norwegian waste recycling companies. The criminal activity appears well organised and many of the perpetrators are repeat offenders.



## Illegal land development threatens nature

Illegal land development takes place by actors clearing land, digging, blasting, filling in, leveling and building in violation of granted permits or without applying to the competent authorities for permission. Waste is also dumped illegally. Recent prosecutions involve many differing and, in some cases, very serious violations of the legislation. It is *likely* that both private individuals and enterprises will commit serious, illegal land development.

Enterprises do not follow construction regulations when expanding their own business premises, building roads and depositing masses and waste without applying for the necessary permits. We have seen in many cases that owners of surplus farm land make deals with contractors to deposit large amounts of waste in unregistered landfills. Some landowners clearcutting their forests without doing the required surveying of environmental consequences, thereby destroying valuable, biodiverse forests.

Construction of land-based wind power plants also leads to large-scale landscape degradation, and several owners of wind power plants have been reported to the police for violation of their permits or environmental interests.

The judgment passed by the Supreme Court in the so-called Fosen case concluded that the construction of a wind power plant violated the UN Convention on civil and political rights.

Private individuals also develop their properties illegally. This ranges from owners of cabins in landscape protection areas and the protected 100m zone along the Norwegian coast who extend and renovate cabins in violation of permissions granted to farmers and cabin owners who build roads for easier access, but to the detriment of moorland and other vulnerable areas.

Waste that is disposed of illegally, whether on land or in the sea, may cause pollution, and may discharge hazardous substances for many years. In several cases, illegal removal of masses and construction are believed to have caused landslides and life-threatening collapse of constructions.

These criminal acts are deliberate and systematic, and may persist for a long time and with very serious negative consequences for both humans and the surrounding natural areas and wildlife. The damage is often irreversible.





## Marine litter from fisheries, aquaculture plants and consumption

Marine litter is a global problem, and plastics make up around 80 per cent of all litter in the ocean. In Norway, consumers and the fisheries and aquaculture industries are the three biggest sources of plastic litter in the sea. It is *likely* that marine littering will increase with increased business activity linked to the sea.

The sea is Norway's most important natural resource. A significant share of marine littering represents violation of the Norwegian Pollution Control Act, and these offences cause great harm and suffering to a range of organisms. Over time, plastics decompose into microplastics, which may harm marine life. Environmental contaminants travel over great distances with the wind and ocean currents. Marine littering is a major challenge in Norway, and the detection risk is low. A lot of litter in the sea comes from businesses which continue their littering even after having been sanctioned.

Littering business enterprises achieve large cost savings by not maintaining their fishing gear or not disposing of waste in accordance with applicable laws and regulations. The main sources of marine littering are abandoned fishing gear, bad weather and acute events that lead to loss of fishing gear, plus discharges from ships and land-based businesses.

In Nordic waters, the aquaculture and

fisheries industries and leisure fishing are responsible for a substantial part of marine littering. Every year, large amounts of fishing gear, including fishpots, are removed from the sea along the Norwegian coast. The aquaculture industry contribute macro-plastics in the form of discarded ropes and equipment parts.<sup>28</sup> Also, abandoned fish farms leave installations, the removal of which the Government has to pay for.

Ships also contribute to marine littering. It has been uncovered that ships dump waste in Norwegian waters. Containers going overboard are also a problem. Worldwide, 3000 containers went overboard in 2020. That year, containers that went overboard led to discharge of large quantities of plastic granulates and paraffin wax along the Norwegian coast. The Corona pandemic has caused a global freight crisis characterised by crew shortages and overloaded container vessels to meet demand and catch up with delays.

The pandemic has also led to an explosive increase in pollution from disposable products, e.g. rubber gloves, face coverings and disinfectant bottles. This is a new type of littering which is particularly visible on beaches and at sea.

In land-based industries, it is especially improper waste disposal that leads to discharges into rivers and fjords.

<sup>28</sup> Højman, Carl; Fabres, Joan; Johns, Hilde R; Sklet, Snorre; Olsen, Julia; Nogueira, Leticia A. & Bragtvædt, Stian, "Makroplast fra fiskeri og havbruk: kunnskapsstatus, forebyggende tiltak og kunnskapsbehov", SALT/Nordlandsforskning & Marfo - Senter mot marin forsøpling, 1:2022.



# Crime against the welfare state

The Norwegian welfare state is designed to ensure everyone equal access to welfare benefits, and is primarily financed by taxes and excise duties on income, consumption and wealth. The model is based on trust and therefore vulnerable to fraud. Reduced trust in the welfare state threatens the foundations of the Norwegian society. Evasion of taxes and excise duties, abuse of benefit schemes and corruption threaten the financing of the welfare state. The tax base will also come under pressure for other reasons, e.g. an ageing population.

Benefits disbursed through the national insurance scheme, i.e. for pensions, sick pay, unemployment and maternity benefits, make up a substantial share of government expenditure. Many of the benefits are disbursed following an automated and efficient case handling process and characterised by a high volume of transactions.

Under the pandemic, a number of temporary benefit schemes were introduced and which were abused by criminals. Some of them were very well organised and succeeded in committing large-scale fraud, particularly of the wages and salaries compensation scheme. Also, it was found that a small number of accountancy

businesses facilitated the frauds.

The investigations have uncovered that a small number of persons with good knowledge of reporting and control functions were able to manipulate the automated application processes and granted benefits on false grounds.<sup>29</sup> Corruption are criminal acts that provide unwarranted benefits. Corruption is theft of political, social and economic benefits from the populace as a whole and represents a threat to the welfare state because it hampers economic development and results in increased risk and cost to lawful business and industry.<sup>30</sup>

<sup>29</sup> Skatteetaten, "Trusselvurdering Covid-19: Hvilke alvorlige kriminalitetstrusler vil Skatteetaten stå overfor ved en normalisering?", 2021.

<sup>30</sup> Regjeringen.no, "Kamp mot korrupsjon", 2009.



## Fisheries crime deprives society of substantial income

Marine resources are very important for value creation along the coast and for the Norwegian economy. Seafood is Norway's second largest export (after oil and gas) with ample opportunities for profit for many of the actors in the business. It is *highly likely* that some fishermen and fish reception facilities systematically under- and misreport fish and shellfish catches.

Fisheries crime undermines competition in the industry, tax and duty revenues and the authorities' resource management.

The large value of fish and shellfish catches in Norwegian waters attract fishermen and businesses who profit from under and misreporting of catches at fish reception facilities. This is done either in collaboration with the fishermen or by the facility themselves misrepresenting the value of the catches to the fishermen. If they collaborate, the facilities compensate the fishermen for the under- and misreporting by paying a higher price for the catches. The facility gets more fish and the fishermen can fish more than their quotas.

Weighing per pallet provides opportunity to manipulate bought and sold notes. Furthermore, production chains facilitate writing off a larger than true share of the produce. Misreporting the species caught also provides

financial benefits for both reception facility and fisherman. The fisherman gets a higher price than the fixed minimum for the reported species, while the reception facility pays less than half price for produce that can be sold at full price in the market. Companies that own several reception facility or control multiple links in the value chain, obscure under and misreporting by moving produce between the facilities. Sale of fish also goes through apparently law-abiding companies without being reported.

Some businesses that systematically under and misreport catches, also employ vulnerable foreign workers who are offered poor living conditions and are subject to unwarranted deductions in their wages. In some cases, business that systematically under and misreport catches outcompete law-abiding businesses and take over market shares and expand their vertical integration.

Vertically integrated actors abuse their market position to achieve gains through systematic sale of illegal catches of fish and shellfish. The MO often involves not declaring sales to the customs and tax authorities.



At a trial in 2021, evidence was presented describing how one fish reception facility over many years systematically had underreported catches and defrauded its customers by selling fishmeal with a lower protein content than stated. In the court's opinion, the underreporting of catches received at the facility and the defrauding of the customers was so large scale and had taken place over so many years that it was endemic to the company.



## Undeclared sale of foodstuffs

Actors in the food industry who do not declare sales and thereby evade paying taxes and excise duties, can take lower prices than law-abiding actors, which leads to distorted competition. Sales of a wide range of foodstuffs go undeclared in Norway. Particularly, shellfish and game are in high demand both in Norway and abroad, and profit opportunities from not declaring these sales are ample. Consumers want to buy their goods as cheaply as possible, while the internet makes illegal sales easier. It is therefore *likely* that illegal sale of foodstuffs will increase.

Illegal sale of food may constitute a health risk since it is impossible to know how the food has been treated. According to Europol, food safety is a growing concern in Europe.<sup>31</sup>

The first quarter export value of Norwegian seafood has never been larger than in 2022. The price of Alaskan king crab has gone up, inter alia because a number of fishing areas off the coasts of Alaska and Canada have been closed, and because Russia has now been excluded from western markets.

Fishermen, both leisure and professional, and reception centres fail to declare all shellfish sales. Undeclared sales of shellfish take place directly between fisherman and consumer, via online marketplaces like finn.no and social media, e.g. Facebook, or with reception

centres as intermediaries.

In the latter case, shellfish is sold to shops, restaurants and hotels.

Shellfish that is sold illegally is generally also caught illegally. In some cases fisherman and reception centre collaborate to underreport king crab catches, thereby covering up illegal fishing.

The prices of some kinds of game meat has also gone up, providing a profit opportunity for people who do not declare sales. As with fish and shellfish, game meat is sold undeclared from private homes and via social media. The meat is distributed around the country, and the police have indications that undeclared game meat is smuggled out of the country.

Ready-made food is also sold illegally. The police have information indicating that persons working illegally in Norway prepare take-away food in private homes to reduce detection risk. Persons with legal residence also choose this MO to work illegally. The food is prepared for sale to private individuals, shops and restaurants, and the sale is agreed via for-purpose Facebook groups.

<sup>31</sup> Europol, "Serious and organised crime threat assessment (SOCTA)", 2021.





## Tax fraud in business and industry

Tax fraud is committed by failing to provide information or providing incorrect information to the tax authorities in order to obtain a tax benefit. The tax assessment system in Norway is based on trust. Both companies and private individuals commit tax fraud. It is *highly likely* that many actors in various industries will continue to underreport or fail to report wages and turnover as these offences are highly profitable and detection risk is low.

Tax and excise fraud is the most common crime in private business and is most common in the construction industry. Nevertheless, tax fraud is committed in all industries and involves undeclared wages, salaries and turnover.

When wages and salaries are not reported to the Norwegian Tax Administration, advance tax deductions and employers' national insurance contribution go unpaid and the state loses income. Some employees report that employers deduct tax from wages and salaries but fail to transfer these to the state.<sup>32</sup> Not declaring wages put employees in a vulnerable situation because they do not earn rights to e.g. unemployment and sickness benefits.

By not declaring sales, companies save income tax and other duties while defrauding the state of income. During the national interagency "Black Week" action against the delivery industry in autumn 2021, inspectors

found many indications of undeclared work and sales. Among the around 100 businesses inspected, inspectors found NOK20 million in unpaid VAT.

Another way of evading taxes is to hide assets in so-called tax havens. Tax havens can be used legally, but can also be used to evade assets from taxation.

<sup>32</sup> A-krimsentret i Oslo, "Arbeidslivskriminalitet i bygg- og anleggsbransjen i Oslo og Viken", 2021.



## Corruption in municipalities

The scale of corruption in Norway is difficult to assess because it takes place in the dark and the persons involved all risk prosecution. Both parties involved in a bribe are therefore interested in secrecy. Although very few cases of corruption have been uncovered in municipalities, the investigations demonstrate that it is *likely* that there is corruption and that it can go on for years without detection. It is *likely* that the risk of corruption is greatest in connection with tenders and the granting of permissions.

In 2021, Transparency International surveyed people's attitudes to and own experiences with corruption in Norway and the EU countries. The main finding is that people in Norway have a high level of trust in the authorities. At the same time, the report emphasises that this trust must be defended. Blind trust and an exaggerated belief that corruption does not happen here are in themselves risk factors.<sup>33</sup>

Norwegian municipalities are characterised by close connections where the employees' financial interests and private relations can lead to conflicts of interest and even corruption. A number of corruption cases, e.g. in connection with tenders, in municipal administrations have been investigated in recent years.

Corruption at the municipal level often takes

place in connection with applications for land development, e.g. of farmland, nature and recreation areas. The involved parties have a mutual interest in keeping the offence hidden.

The risk of corruption is particularly high in public tender processes, which are particularly prone to bribery. Private gain and winning public tenders can motivate corrupt acts by both buyer and supplier.<sup>34</sup>

Corruption in municipalities may have serious negative impact on nature, business and industry and people's trust in the public sector.

<sup>33</sup> Transparency International Norge, "Global corruption barometer i Norge sammenlignet med EU-landene", 2021.

<sup>34</sup> Transparency International Norge, "Domssamling 2020", 2021.



# Offences against animal welfare

Animals have an intrinsic value independent of their utility to humans, must be treated well and protected from unnecessary stress and strain. Beating animals, putting them in a situation of helplessness, performing sexual acts on them and using live animals as bait or feed is prohibited.<sup>35</sup>

Pets, leisure animals and livestock are totally at the mercy of humans and their treatment of them. They are silent victims and it is believed that violent and sexual acts and maltreatment of animals largely goes unreported.

The demand for pets increased during the pandemic<sup>36</sup>. This trend turned in autumn 2021, when animal welfare organisations reported that many animals were being dumped by their owners and that owners were trying to find new homes for their pets. Digitalisation also affects animal welfare in that photos and videos are shared and persons who are interested in committing violence or sexual acts on animals find a meeting place.

In autumn 2021, the police received more reports than usual about maltreatment of animals. Many owners have health and mobility problems due to alcohol and drug addiction, old age and mental issues. A few are obsessi-

ve hoarders and house dozens of cats. A number of the perpetrators are repeat offenders.

The welfare of aquaculture livestock is being criticised. In 2021, a record number of farmed salmon – 54 million – died before the time of slaughter. Also, close to 41 million cleaner fish, which have a near 100% death rate, was released into netpens in 2021. Both salmon and cleaner fish experience crowding and thermal and chemical delousing as stressful. This also damages their gills, fins, eyes and skin and is a great problem for their welfare.<sup>37</sup> Being moved from one netpen to another also increases risk of injury and death.<sup>38</sup>

It is also a problem for animal welfare that fishing nets and fishpots are abandoned to so-called ghost fishing. It has also been uncovered that fishermen cut the wings off live rays and throw the fish back into the sea.<sup>39</sup>

<sup>35</sup> Animal Welfare Act section 14.

<sup>36</sup> E24, Kraftig omsetningsbutikk for dyretjenester, 2021.

<sup>37</sup> Veterinærinstituttet, "Fiskehelse rapporten 2021", Rapport 2a/2022.

<sup>38</sup> NTAES, Havbruk og fiskeri – verdikjeder, ansvar, lovbrudd, 2021.

<sup>39</sup> Dagbladet, "Dansk fiske avslørt: - Helt forkastelig", 2022.



## Maltreatment of livestock

Private individuals, animal welfare organisations and the Norwegian Food Safety Authority all report maltreatment of livestock in Norway. It is *likely* that some farmers with reduced capacities due to mental health issues will maltreat their livestock.

The police all over the country receive reports about maltreatment of livestock. A number of cases of dead sheep and cattle have been uncovered, and in the most serious cases dozens of dead animals have been found on the farm. The maltreatment consists of e.g. failing to feed and water the animals, clean their pens and care for them. Animals are also found that are in such poor condition that they have to be put down on the spot.

Continued maltreatment over time is also a substantial problem. There are farmers who over many years have been unable to properly care for their livestock and fail to comply with orders from the Norwegian Food Safety Authority. Many avoid being banned from having animals by improving care while under supervision.

Activists have uncovered a number of farms where pigs are kept in overcrowded pens with nothing on the concrete floor but faeces, and injured pigs and weak animals that should have been secluded from the others.<sup>40</sup> There are examples of food producers who stop

taking deliveries from farmers due to maltreatment of livestock.

Good animal husbandry is also difficult during the long and cold Norwegian winter, and there are examples of farmers who do not bring their livestock down from mountain pastures, where they suffer from lack of food, water and protection from the elements when winter sets in. Also, some farmers fail to provide animals with a dry spot on which to lie by failing to drain and/or spread sawdust on the ground.

Information in some of the reports indicates that some farmers may be unable to care for their livestock due to illness.

<sup>40</sup> NRK, "Griseindustriens brutte løfter", 2021.



## Violence and sexual acts against animals

Digitalisation has eased contact between people who want to maltreat or have sex with animals and for them to share photos, videos and animals. It is *highly likely* that animals will be subjected to violence and sexual acts in Norway and that many of these cases will involve serious abuse.

In 2020, the police uncovered an organised network of people who systematically abused dogs sexually. Many of the members of the network were sentenced to fines and prison for these acts in 2021. In addition to repeatedly assaulting the dogs sexually over several years, the dogs were also generally maltreated. Many of the acts were aggravated, involving rape and penetration with objects.<sup>41</sup>

Some farmers and horse owners have also experienced that outsiders sexually abuse their cows, goats and horses. This happens both when the animals are penned up and when they are out on pasture.

The perpetrators are mostly men but there are examples of women and children sexually abusing animals. It is quite common that men who commit or who have photos and video clips of sexual abuse against animals, also are in possession of child sexual abuse material. A few have also previously been reported to the police for ordering live-streamed sexual abuse of children, incest and sexually degrading

treatment of humans.

The police also receive a large number of tip-offs about violence against pets. The perpetrators are often alcohol and drug addicts or mentally ill people who maltreat their dogs or cats. Cats appear to be particularly popular targets of torture and being shot and killed. Some maltreat pets to be nasty to other family members.

In a very few cases, the perpetrators of violence against animals have been minors who often share their acts on social media. This may involve killing birds with knives or bare hands, or maltreatment of cats.

<sup>41</sup> TV2, Massive overgrep mot hunder i to tiår, 2021.

# Virtualisation

The virtualisation and digitisation<sup>42</sup> of the consumer sphere, critical infrastructure and public and private services is speeding up. The internet of things (IoT), 5G, artificial intelligence (AI) and virtual and extended reality give us smart cities, houses, businesses and services that will contribute to progress. Increased virtualisation and digitisation require more minerals and energy, the control of which is of strategic importance.

The market for virtual assets is growing rapidly. Decentralised finance (DeFi) has made it possible to lend money and earn interest on one's cryptocurrency holdings and to pledge them as security for loans. In the future it will be possible to pledge other assets, e.g. non-fungible tokens (NFTs).<sup>43,44</sup>

Virtual worlds, so-called metaverses, have existed in online games for many years, but they are expected to become more common as the technology becomes more widespread. Participation in games and other online communities is growing.<sup>45</sup> It is possible to buy and sell goods and services in virtual worlds

like in the physical, and, like in the physical world, there is crime.

We will probably see increased use of so-called digital twins, i.e. digital copies of the real world. This will be useful in simulations, surveillance and administration. It is possible to recreate an office, a factory and whole cities. It is also possible to make a digital representation of a person. This opens many new opportunities for progress and more efficient use of society's resources but also for new vulnerabilities and challenges, e.g. cyberattacks.

Criminals increasingly use advanced technologies and tools available for sale online,

<sup>42</sup> Data are migrating from analogue to digital storage.

<sup>43</sup> A non-fungible token (NFT) is a cryptographic proof of ownership that can be used to prove ownership of e.g. a picture, ticket or game token.

<sup>44</sup> Medium.com, "Introducing JPEG'd: DeFi Meets NFTs", 2022.

<sup>45</sup> DNV, "Introduction to technology outlook 2030", ukjent.



e.g. deepfake technology.<sup>46,47,48</sup> Virtual<sup>49</sup> and cryptocurrencies<sup>50</sup> open new possibilities for financing criminal activities and money laundering. There is also a strong correlation between increased use of cryptocurrency and developments in the field of ransomware attacks.<sup>51</sup> Criminals sell goods illegally on the darknet and new communication and trading platforms are used for planning and committing crime.

Rapid development of quantum technology may present both opportunities and challenges with respect to encryption. Democratization of advanced algorithms, i.e. increased availability without requiring large investments or advanced skills, provides opportunities for

both police and threat actors which previously were exclusive to states.

A more digitised world has also given people on the fringes of society access to likeminded people on various online forums. Many also base their opinions and ideology in conspiracy theories.<sup>52</sup> Also, in an ever more virtual and digitised world large groups of society, e.g. senior citizens, will not be able to master the new technologies.

<sup>46</sup> Etterligning av personers tale eller opptreden på video.

<sup>47</sup> NSM, "Nasjonalt digitalt risikobilde 2021", 2021.

<sup>48</sup> FFI, "Samfunnsutvikling frem mot 2030", 2021.

<sup>49</sup> A virtual currency is a digital representation of value issued by a private actor and not a central bank or other public authority.

<sup>50</sup> A cryptocurrency is a virtual currency that applies cryptography to secure transactions.

<sup>51</sup> Europol, "Cryptocurrencies: Tracing the evolution of criminal finances", 2021.

<sup>52</sup> PST, "10 år siden 22. juli – Sentrale utviklingstrekk innen høyreekstremisme", 2021.



# Financial crime in the virtual age

The virtualisation<sup>53</sup> of society has created new opportunities for criminals. Digital crime takes place without physical contact on virtual platforms, often involving the use of fake and stolen identities. Digital theft and fraud are also often carried out without the perpetrators ever setting foot on Norwegian soil.

Europol expects criminals to increase their use of artificial intelligence and so-called deepfakes in the coming years. By applying artificial intelligence to existing MOs, attacks on enterprises and private individuals can be carried out on a far greater scale. Artificial intelligence may also result in better translations, making fake emails more convincing. Robots and artificial intelligence (AI) can also be used to manipulate markets.

There is a reported increase in criminal networks attacking Norwegian bank customers. While prior to the pandemic such attacks were conducted by three to five networks, there are now 15 to 20 active networks. International criminal networks also exploit vulnerable persons by using their IDs to take out loans. The perpetrators are willing to use threats and violence and work closely with criminal networks in Norway.<sup>54</sup>

New digital banking solutions enable rapid, cashless money transfers.<sup>55</sup> The main problem

with digital payment solutions is that the anonymity and speed of the international transfers make tracing the flows difficult. This probably makes it easier for criminals to conceal cross-border transactions, beneficial ownership and incomes and assets abroad, incomes and assets that may have illegal origins. This also makes digital payment solutions suitable for money laundering. The same issues apply to virtual currencies. Although tracing virtual currencies can be easy, it is also becoming easier to apply methods to prevent tracing.

<sup>53</sup> An increasing number of things, including data storage, retailers and assets, are no longer physical, but virtual, and available in digital space.

<sup>54</sup> DNB v/FC3, "Annual Fraud Report 2021", 2022.

<sup>55</sup> FATF, "Guidance on Digital Identity", 2020.



## CEO fraud

CEO fraud involves perpetrators posing as managers who contact subordinates in an enterprise or organisation to manipulate them into transferring large amounts or approving disbursements. The request to make the transfer or disbursement may be made via email or telephone. The latter method is often applied more surgically and in major, more complex attempts at CEO fraud. It is *highly likely* that available new technology, such as deepfake, will increasingly be used in attempted CEO frauds targeting major enterprises.

CEO fraud is a form of fraud that in some cases, in particular when targeting large international enterprises, can generate substantial proceeds. There are several cases of Norwegian enterprises being defrauded of a hundred million NOK or more. The same MOs have also been used in cases involving smaller amounts. Several NGOs, charities etc. have been victims of such attacks, suffering losses of tens of thousands of NOK.

Europol reports that the pandemic has been a catalyst for invoice and CEO fraud. The criminals have become more sophisticated and surgical in their attacks. The perpetrators find the optimal time to strike, use correct wording

and apply AI very effectively. The laundering of the proceeds is also very professional.

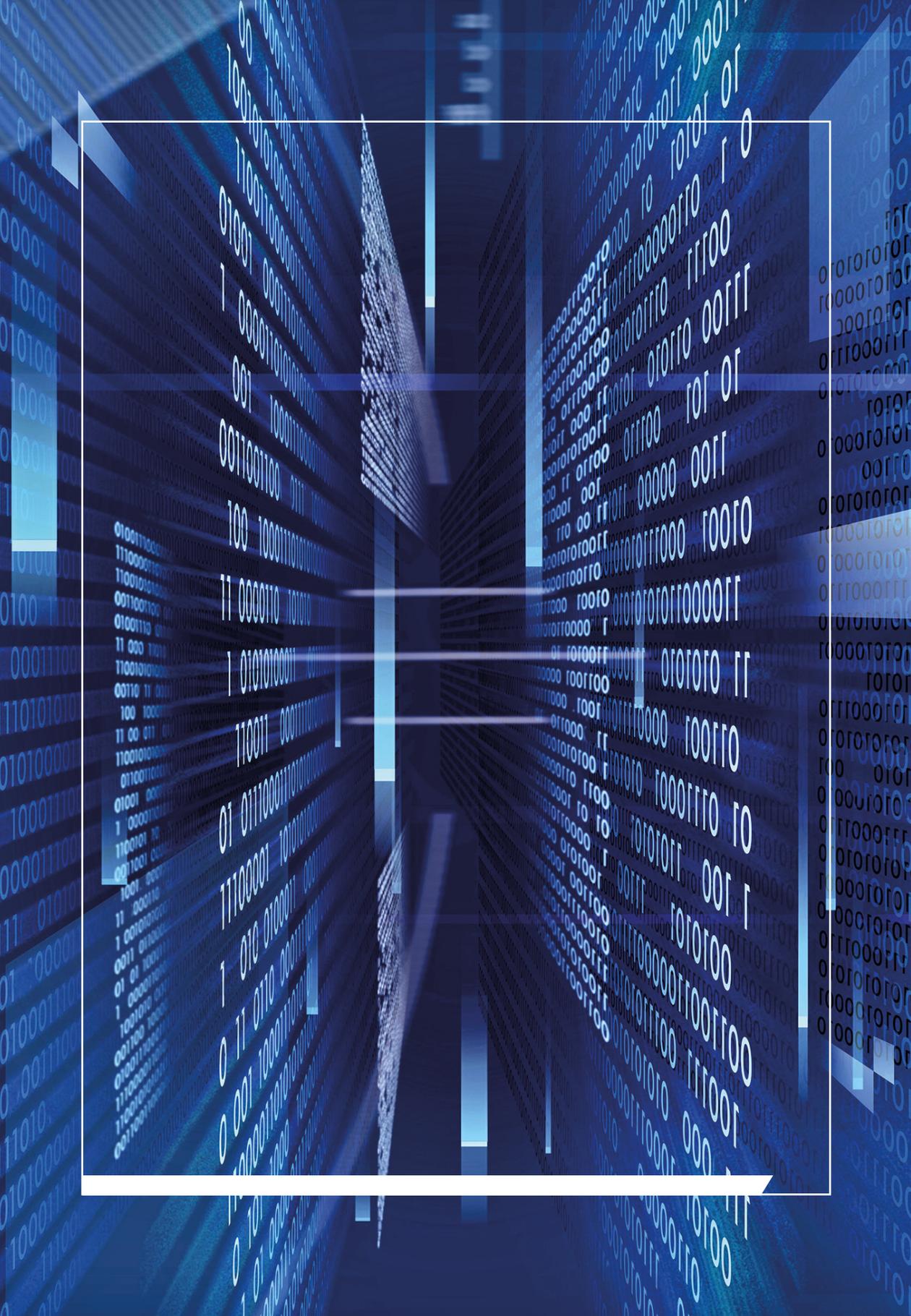
In some cases, the perpetrators use an approach that is precisely tailored to the target. One MO is targeting executives and board members presumed to have access to corporate bank accounts, with the perpetrators posing as representatives of the Norwegian ID verification service BankID. The attacks often take place in connection with a real event in the enterprise, such as changes to the company registration, with the victims being told to approve the changes via BankID.

In reality, such approval gives the perpetrators access to the corporate bank account. The Norwegian bank DNB reports that the perpetrators appear to be very professional and well prepared.<sup>56</sup>

According to the Norwegian Business and Industry Security Council, 9 per cent of Norwegian enterprises are victims of CEO fraud or fraud attempts every year. The attacks are equally common in the private and public sectors, but small enterprises are more likely to become victims of CEO fraud attempts than large enterprises.<sup>57</sup>

<sup>56</sup> Dagens Næringsliv, "Ny svindelmetode lurer direktører og styreledere til å åpne bedriftskontoen: - Internasjonal organisert kriminalitet med norske medhjelpere på bakken", 2020.

<sup>57</sup> Næringslivets Sikkerhetsråd, "Kriminalitets- og sikkerhetsundersøkelsen (KRISINO)", 2021.





## Money laundering using virtual assets

Virtual assets will probably become more common in both online games and in art and finance. This opens new opportunities, but also creates new problems. It is *likely* that virtual assets increasingly will be used to launder money.

It is estimated that USD 8.6 billion were laundered via cryptocurrencies in 2021, an increase on previous years. This makes up just a small fraction (0.15 per cent) of the total cryptocurrency transactions made in 2021<sup>58</sup>, but this figure only includes detected money-laundering transactions.

The laundering of proceeds from traditional drug crime and other organised crime is unlikely to be detected to any great extent, as they will mostly appear to be legal transactions between two persons.<sup>59</sup>

There is a relatively small number of foreign exchanges which receive the majority of the known proceeds laundered via cryptocurrencies. They often use the infrastructure and liquidity of larger exchanges, but are themselves responsible for checking customer information and the origin of the funds. These checks are often very deficient. It is also a problem that

many of the major international cryptocurrency exchanges reside in jurisdictions known for lack of transparency and oversight. Some exchanges occupy premises in the same office building in Moscow and have laundered huge amounts linked to Russian criminals.<sup>60</sup>

NFTs<sup>61</sup> are another type of virtual assets that can be used to launder money. In the future, NFTs may be used in a significantly greater range of applications. For instance, it can enable artists to demonstrate ownership of music or videos, allowing them to sell their works and services directly to the fans. NFTs are also used by criminal actors. There are several examples of people buying "fake" NFTs. In practice, this means that you are buying a copy from another provider, comparable to buying pirated clothing brands. In this connection, the fraudsters often carry out fake transactions, so-called wash trading, making the NFTs appear to be popular and frequently traded. There are indications that wash trading has increased significantly in 2021.

<sup>58</sup> Chainalysis, "The 2022 Crypto crime report", 2022.

<sup>59</sup> Europol, "Cryptocurrencies: Tracing the evolution of criminal finances", 2021.

<sup>60</sup> Bloomberg, "Ransomware HQ: Moscow's tallest tower is a cybercriminal cash machine", 2021.

<sup>61</sup> A non-fungible token (NFT) is a cryptographic proof of ownership that can be used to prove ownership of e.g. a picture, ticket or game token.



## Increased use of money mules

A money mule is a person who receives money, digitally or in cash, from one person and transfers it to another against payment. Money mules often transfer money for fraudsters to foreign bank accounts. The use of money mules is increasing in many countries. Money mules are commonly used in connection with digital for profit crime, and it is therefore *likely* that we will see an increase in the use of money mules in Norway in the coming years.

Denmark recorded a 400 per cent increase in the number of detected money mule accounts from 2018 to 2020.<sup>62</sup> In Norway, one of the largest banks reported that it had rejected 1500 customers in 2021 due to suspicion of money laundering, fraud and money mule activities. This is an increase from 2020 and a continuation of a long-standing trend.<sup>63</sup> Økokrim is also seeing an increase in the number of reports of money mule activity in the last five years.

Europol reports how online dating and social media are increasingly being used to recruit money mules. Adverts promising quick and large profits are used to entice people into making their accounts available. There are also reports from the UK of an increase in the use of

younger people as money mules.<sup>64</sup>

There are three main types of money mules. The first are young people who do this in return for money or luxury goods. Many of them probably do not realise the gravity of what they are doing. The second are people living alone, in many cases elderly people. They are often unaware that they are being exploited. The third are people in financial difficulties who are more inclined to say yes to making easy money, or who are pressured into making their bank account available in order to pay outstanding debts.

Young people appear to be recruited as money mules to a greater degree than others. One MO noted by Økokrim is young people being recruited into what they believe is a chance to exploit the recruitment bonuses offered by online betting companies. In reality, the money they receive – and forward – stem from crime. There are also several reports of relatively young people receiving money from fraud and then laundering it by buying expensive watches.

<sup>62</sup> TV2, "Metodene er utbredt i Sverige og Danmark – frykter den skal spre seg til Norge", 2021.

<sup>63</sup> Dagens Næringsliv, "Kraftig økning i kunder som kastes ut – DNB har avvirket 1483 kundeforhold i år", 2021.

<sup>64</sup> NCA, "National Strategic Assessment of SOC", 2021.



# Digital crime

Almost 19,000 cases of fraud were reported to the police in 2021. Most of them were committed online. Online and computer fraud is the new burglary and the crime people are most likely to become victims of. In coming years, fraud attempts are expected to become automated and more tailored to the individual victim.<sup>65</sup>

Digital crime is in many cases mass fraud attempts distributed to many potential victims. The actors are often criminal networks, both foreign and domestic. Europol reports that criminals are increasingly using compromised information from computer hacking to tailor their attacks. By combining information about the target with the ability to pose as someone else, the likelihood of succeeding with the fraud increases significantly.<sup>66</sup>

Social manipulation is often a key element in fraud. This means posing as someone other than who you really are. One commonly used method is the perpetrator using services which display the phone call or text message as coming from a number of the perpetrator's choosing, so-called spoofing.<sup>67</sup> According to Europol, elderly people are more often subjected to fraud attempts that combine social manipulation and technical elements. The use of technology enabling the perpetrator to remotely control the victim's computer is

particularly common.

Økokrim has also seen several cases of fraud committed via digital marketplaces such as Facebook Marketplace and Finn.no, with sellers receiving payment for goods that are never delivered.

There are also regular fraud campaigns at various times of the year, often in connection with vacations, holidays and retail sales campaigns. Leading up to Christmas, many people receive text messages or emails from perpetrators posing as legitimate delivery service providers. The text message will often claim that a parcel is on its way, but that a minor fee must be paid before delivery. In reality, the aim is to gain access to the card information and defraud the victim of several thousand NOK.

<sup>65</sup> DNB, "Årlig Trusselvurdering", 2021.

<sup>66</sup> Europol, "Internet Organised Crime Threat Assessment (IOCTA) 2021", 2021.

<sup>67</sup> Spoofing means that the person receiving the call sees the number the perpetrators want them to see.



## Investment fraud

Investment fraud entails being deceived into investing in projects and products that are worthless or non-existent. This may be investments in cryptocurrency, shares or other financial instruments, property, commodities or valuable objects such as art and antiquities. Manipulation of victims is an essential part of the fraud process. It is *highly likely* that investment fraud involving cryptocurrencies and trading platforms will increase, and that Norwegians, in particular men aged 60 to 80, will be defrauded of significant amounts.

According to Europol, there is an increasing trend in investment fraud for victims to be defrauded several times. First, they are duped into making the investment itself, then they pay for help to regain the money without realising that it is the same perpetrators who are out to take them for another ride. This development has also been seen in Norway.

In recent years, investment fraud through sale of cryptocurrency has increased. The methods are legion. Some MOs are the same as those seen in share investment scams. Other MOs include creating fake online trading platforms, often combined with aggressive marketing on social media and fraudulently using celebrities to appear legitimate. Victims may also receive fictitious receipts and documents showing investments and profits, which

are then used to manipulate the victim into making further investments.

Økokrim estimates that Norwegian fraud victims transferred around NOK 75 million out of Norway in connection with cryptocurrency fraud in 2021. Globally, losses from cryptocurrency fraud increased by around 81 per cent in 2021 from the previous year. The number of defrauded persons appears to be lower, but the average loss in each case appears to be higher. There is a major increase in the number of so-called rug pulls, i.e. investment projects where the developers steal the invested capital. Many of these cases are in connection with decentralised finance (DeFi) projects.<sup>68</sup>

Ponzi schemes are a form of investment fraud that attract investors with the promise of high returns. Ponzi schemes are rarely traded in the open market, making them harder to detect. Økokrim has received information about several Ponzi schemes in Norway. Some of the organisers are known from similar schemes in the past.

<sup>68</sup> Chainalysis, "The 2022 Crypto crime report", 2022.



## BankID fraud

The police regularly receive reports of fraud during which the perpetrators have gained access to the victim's online bank. Some of the fraud campaigns are hard to uncover, but the perpetrators mostly target victims with low digital expertise, such as the elderly. The technology is relatively easy to acquire, but using it requires some expertise. However, once you have that expertise, it is easy to teach to others. It is *highly likely* that criminal actors will continue to target the elderly, while new technology will make such fraud more effective, also against other groups.

The MO often involves the victim being called from a spoofed telephone number. The perpetrators pose as representatives of the bank or the police, telling the victim that unauthorised persons have gained access to their bank account. They then talk the victim into giving up control of their online bank by approving access using the electronic identification provider BankID, and then they empty the bank account. The money is usually moved via mule accounts. There are also reports of perpetrators posing as the police of other Nordic countries.

There have also been several cases where victims have been called by someone posing to be from Økokrim. The perpetrators provide a fictitious employee number and the telephone number they call from is similar or identical to Økokrim's own number. The perpetrators then

provide a false explanation for why they are calling, often along the lines of irregular activity on the account, and offer their assistance. The victim is then asked to provide personal details and approve the BankID verification on their telephone. The perpetrators then empty the account.

In summer 2021, a fraud campaign targeted young people looking for a place to live. The victims, mostly students, had advertised for flats to rent. They were then contacted by the perpetrators via text messages with an invitation for a showing. The invitation required following a link and logging in with BankID to confirm the appointment. In reality, this process enabled the perpetrators to access and empty their online bank accounts.

One problem that emerges following BankID theft and the use of spoofed telephone numbers, is the erosion of trust in key infrastructure. BankID is currently used by several Norwegian public databases and services, including the Labour and Welfare Administration (NAV), the Tax Administration and public health services. If it becomes hard to distinguish between legitimate and fraudulent use of BankID, this will quickly cause problems in the communication between the public sector and the general public.

# Glocalisation

Cultural, financial and political globalisation has local consequences. The same applies to crime. Crime committed in one country may have local consequences elsewhere. The physical distance to the actual victims of crime, be they people, animals, businesses or nature, also creates an emotional distance to the acts.

Globalisation has made national borders less important. Norwegian nationals shop from foreign websites, paying through foreign payment service providers. Norwegian companies set up businesses abroad, and foreign companies compete for tenders in Norway on an equal footing. Cross-border activity is becoming more common and cross-border financial transactions are carried out faster and faster. However, the pandemic uncovered major weaknesses in the global business model, and regionalisation is expected to increase going forward.

A small number of major corporations now dominate entire value chains and sectors and have become key players in the international economy. The business model of international mega-corporations calls for outsourcing production to locations where the labour and environmental costs are the lowest. Services are also outsourced, and the majority of large Norwegian businesses now depend on foreign companies for IT support.<sup>69</sup>

**So-called beaching, where obsolete ships**

**are run aground on beaches in Asia and broken up for scrap, is another example highlighting the environmental problems of globalised markets,** as is untrained labour being attracted to Norway by relatively high wages. When raw materials are extracted in one location, processed in another and the resulting components assembled in a third location, this also results in large-scale transport activities with an environmental impact.

More international business and industry also results in more foreign ownership of Norwegian businesses and more foreign businesses being active in Norway. If foreign contractors are added to this mix, Norwegian expertise and local business development may suffer. Foreign acquisition of Norwegian businesses may also reduce taxable income in Norway and result in jobs and technology moving abroad.

However, a stronger focus on national priorities among several of the major world economies is now challenging the global economy that has been built up on low trade

<sup>69</sup> NSM, "Helhetlig digitalt risikobilde", 2019.



barriers, strong global investment and responsible fiscal management. States increasingly view problems and opportunities in a unilateral and local perspective, and trade has become an instrument of rivalisation.<sup>70</sup> Brexit<sup>71</sup> is one example of this.

At the same time, the EU is strengthening its joint framework and regulations, also in the money-laundering area, and has set up a dedicated unit within Europol to combat financial crime in Europe. Problems relating to secretive bank havens and exchange of information with countries that facilitate hidden ownership of enterprises and property remains, however, a key weakness of the authorities' ability to uncover and investigate cross-border crime.

The coronavirus pandemic is still ongoing and will make itself felt for years to come. Several countries are experiencing a financial downturn and inflation and interest rates are expected to rise, which will make it harder for highly indebted countries, enterprises and people to service their debts.

Globalisation is expected to continue, but in some areas and in some countries, it appears that the world is moving towards formation of blocks and a more regional focus. One example of this is payment systems. Russia's exclusion from SWIFT will accelerate this trend.

<sup>70</sup> World Economic Forum, "The Global Risk Report", 2020.

<sup>71</sup> Storbritannia gikk ut av EU 31. januar 2020.



# Cross-border crime

Cross-border crime and actors follow on the heels of increased globalisation and economic integration.

Internationally, serious environmental crime is to a large extent the work of criminal networks, often with links to other serious and organised crime. Environmental crime can be perpetrated by the same actors – using the same methods and transport routes – that engage in illegal arms trafficking, drug smuggling and human trafficking.

Corruption, money laundering, document forgery, tax evasion and customs fraud are other forms of crime that often take place across borders. The international aspect is often a driver, as crime is easier to conceal and harder to uncover when taking place across jurisdictions.

Globalised industries, e.g. fisheries, attract criminal networks from abroad. Fish and fish products are Norway's second-largest export commodity, with a total value of NOK 120.8 billion in 2021. In recent years, there have been examples of foreign criminal networks committing fisheries crime through ownership in fisheries enterprises in which they often control several links in the value chain, hide behind complex networks of shell companies and ownership structures in secretive tax havens and shift assets between companies. We have also seen examples of Norwegian actors

committing fisheries crime abroad.

Of particular concern is that many of the major fraud actors who target both Norwegian private individuals and enterprises operate from abroad and make several hundred million NOK from the frauds.

Foreign seafood importers are also subjected to fraud when trying to buy Norwegian seafood. In these cases, both perpetrators and victims are most likely foreigners. By copying Norwegian websites to defraud potential customers they harm the reputation of the Norwegian export industry. Such cases may also involve misuse of the identity of employees and owners in Norwegian seafood enterprises, which in turn may have serious repercussions for those individuals.



## Green transition crime

The green transition is about converting the energy system from non-renewables to renewables to cut greenhouse gas emissions and achieve the goals of the Paris Agreement.<sup>72</sup> The transition will force climate measures and adaptation to climate change that will result in wholesale changes to the way we live our lives. Stricter regulation of sources of pollution and use of natural resources is also expected. Innovation and technology development are key to realising new low-emission solutions and renewable energy. This will require major investments. In order to accelerate the green transition, governments will introduce subsidy and incentive schemes. Government financing schemes and tenders to promote the shift to a green economy will *highly likely* be exploited by Norwegian and foreign actors.

According to Europol, criminals will attempt to profit from the green transition by preparing complex cross-border fraud schemes targeting energy and green certificate investments.

Norway has generous subsidies for environmental and climate-related measures and these schemes may be exploited. Evasion of VAT in connection with climate quota trading which was common a few years ago, is one example

of how some exploit green transition incentive schemes. It was uncovered that small businesses with few employees were trading climate quotas worth several hundred NOK without reporting it to the authorities.<sup>73</sup> The exploitation of the Skattefunn tax reimbursement scheme and fraud involving covid-19-related subsidy schemes are other examples of how such schemes attract criminals.

The renewable energy sector is a rapidly growing international market that attracts capital and investment. The development of renewable sources of energy will require enormous investment, resulting in the green sector becoming entwined with the financial sector. Major development projects require tender processes, both when surveying land for development and during the construction itself. These are corruption risk factors.

The financial loss from wrongfully awarded public subsidies is primarily suffered by the state, but the development of renewable energy may also be hampered by such practices. Large-scale abuse of incentive schemes may also undermine the credibility of important climate measures and distort competition.

<sup>72</sup> Regjeringen, "Det grønne skiftet", 2021.

<sup>73</sup> Økokrim, "Er de kriminelle blitt miljøbevisste?", 2013.



## Norwegian enterprises face increased risk of corruption abroad

Corruption is a global problem and the majority of the world's population live in countries where corruption is rife.

Europol estimates that 60 per cent of European criminal networks are involved in corruption. They pay bribes both to obtain influence and to infiltrate the public and private sectors.<sup>74</sup> It is *likely* that increased competition for resources and scarcity of transport will raise the risk of corruption for Norwegian enterprises abroad.

Norwegian enterprises are expanding into and exporting goods to countries with structural corruption problems. Increased pressure on natural resources may also increase competition for resources and the risk of corruption. This development has been observed in the fisheries industry, where Norwegian enterprises have been involved in corruption to win fishing quotas off the coast of Africa. Overfishing in those areas is believed to have been so extensive as to deplete fish stocks.

Norway also imports goods transported in containers. Prior to the pandemic, corruption was one of the major crime threats in port operations.<sup>75</sup> The pandemic has resulted in lack of containers, delayed deliveries and increased transport costs in the retail industry.<sup>76</sup> This may increase the risk of corruption in ports. Chan-

ged trade routes between Asia and Europe as a result of the war in Ukraine may also raise transport costs and impact corruption risk.

Corruption abroad may be difficult to uncover, as the relevant transactions often go through several links and companies and professional facilitators are used. Transactions are, to a greater degree than before, concealed through legitimate enterprises rather than through shell companies and fictitious consulting contracts.

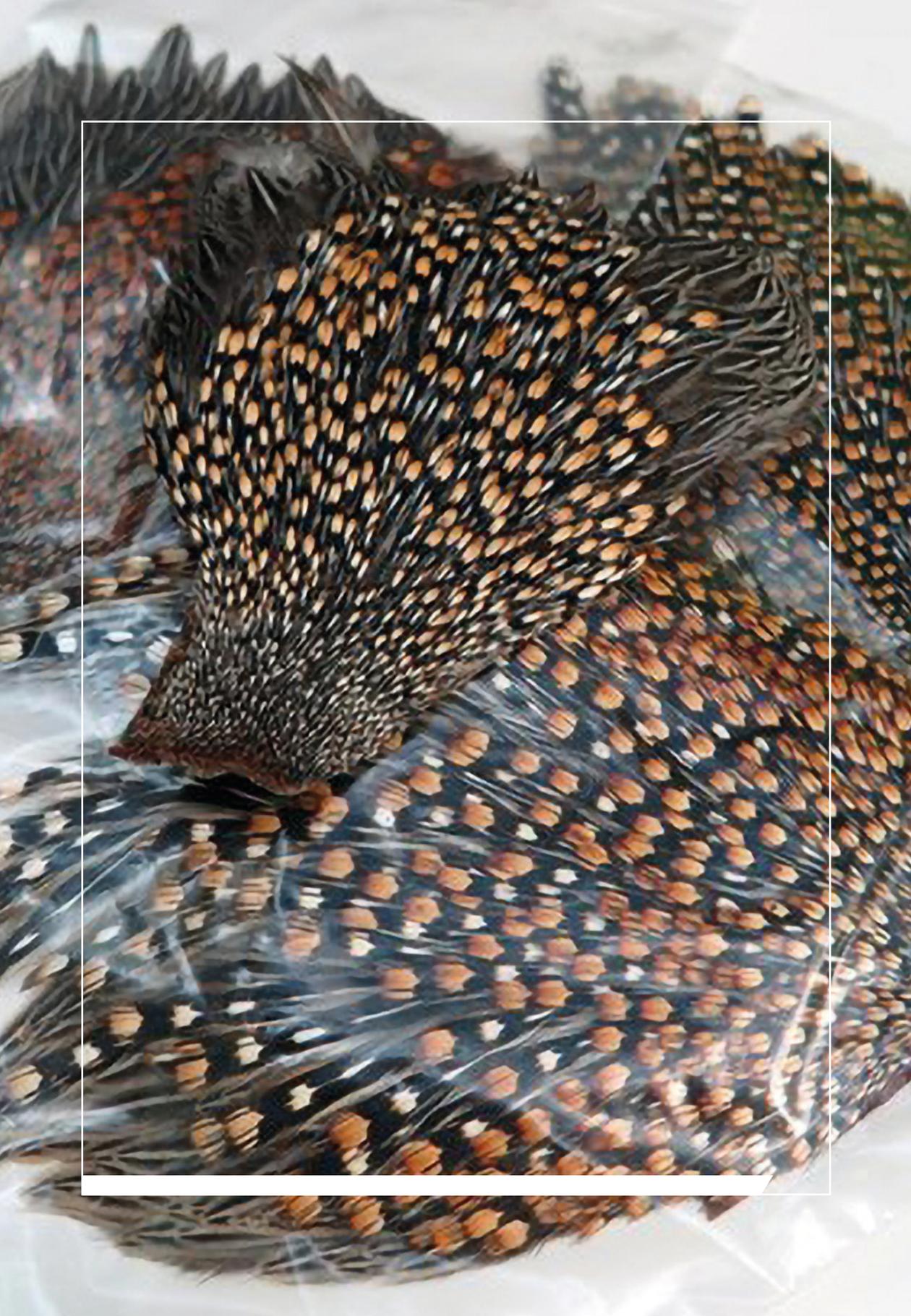
Through an amendment that came into force in 2021 Norwegian enterprises can now be held liable for corruption and other financial crime committed by foreign nationals on behalf of Norwegian enterprises, even if the crime was committed abroad. This means that Norwegian enterprises operating abroad will have to comply with Norwegian standards there as well.

Norwegian business and industry has become more alert to the fact that corruption may exist in the countries where they do business. However, we do know that corruption takes place, in particular in connection with export agreements between Norwegian and foreign companies, in countries where corruption is rife.

<sup>74</sup> Europol, "Serious and organised crime threat assessment (SOCTA)", 2021.

<sup>75</sup> Deloitte, "Fighting corruption in the Maritime Industry", 2015.

<sup>76</sup> NRK, "Mangel på fraktcontainere fører til varemangel og prishopp", 2021.





## Illegal trading in endangered species<sup>77</sup>

Illegal trading in threatened species is transnational and a growing problem globally. This trade is considered an important factor in the extinction of species and populations, which then results in ecosystem destruction. Deforestation and species loss also drive climate change. It is *highly likely* that Norwegian actors will import threatened species to Norway.

Both legal and illegal trade in wild animals and plants are a significant risk factor for the spread of zoonotic diseases. The covid-19 pandemic and bird flu are examples of this.

International nature and wildlife crime mostly takes place under the auspices of organised criminals and the profit potential is considerable. Globally, trade in threatened species is an industry worth billions which has been characterised by the UN as "serious organised crime".<sup>78</sup>

The trade in threatened species includes living and dead animals and plants, and derivative products. Animals and plants are sought after as trophies, food, clothing, accessories and pets, and for use in traditional medicine etc. The trade flows mainly go from countries

in the south to wealthy buyers in the north. In many countries, this trade is a threat to national security and an obstacle to social and economic development.

Some species and products catch a very high price in the black market. Organised criminals use the same routes and methods as for trafficking other illegal goods, and they exploit weaknesses in law enforcement and the courts. Seen in isolation, cases involving import or export of animals and plants may appear trivial, but the total volume makes this a serious crime. For the animals, the trade often causes major suffering and death.

Norway is primarily a market for the purchase of such products, but it is also country of transit and origin. Birds of prey and their eggs are exported from Norway, while reptiles, snake and crocodile leather products, exotic woods and ivory and feathers for making fishing flies are imported, making Norwegians part of the international trade in threatened species. It is also known that foreign nationals participate in organised, illegal hunting for threatened species in Norway.

<sup>77</sup> Illegal trading in animals and plants threatened by extinction involves illegal hunting, harvesting, transport and smuggling of protected and threatened species, as well as trading in derivative products.

<sup>78</sup> United Nations, "General Assembly resolution 69/314 - Tackling Illicit Trafficking in Wildlife", 2015.



## Foreign actors illegally harvest and smuggle species from Norwegian fauna

Norway has a rich flora and fauna, with many species that are sought after for trade, food or collectors' items abroad. It is *likely* that foreigners will engage in illegal tourist fishing and harvesting of birds in Norway and smuggle their catches abroad, and that this activity in some cases is organised.

The price of Norwegian seafood makes smuggling attractive, both for own consumption and sale.

During the summer months, European tourists are regularly caught overfishing and later trying to export the catch without declaring it.

There is a large international market for rare birds, eggs and butterflies. Northern Norway is an attractive destination for bird lovers foreign and domestic, partly due to the rich Arctic bird-life. Eggs and chicks from rare birds are also often smuggled out of Norway. The birds and eggs are taken from nests, and criminals can profit greatly from selling them to international collectors.

Foreign actors also target other species. In 2019, two foreign nationals were arrested and charged with illegally catching protected but-

terflies in Norway. They had travelled around Europe to catch rare and threatened species. In 2021, three Italian hunters were stopped when leaving Norway with 2027 frozen thrushes. 41 of them were of protected species that are illegal to hunt in Norway. The hunters stated that they had hunted in Norway for many years.

Both Norwegian and foreign providers facilitate hunting and fishing by letting hunting rights, vessels and accommodation with freezers. Some of them violate regulations by allowing tourists to exceed quotas. There have also been reports of misrepresentation of catches and providers helping tourists sell their catches.

The consequences of illegal hunting and fishing of species from Norwegian fauna include reduced biological diversity. In some cases, these activities can push species to the brink of extinction. Hunting and fishing are subject to strict quota requirements to allow scientists to form a sound basis for estimating the size of populations and ensure their continued existence.



In some cases, the tourist fishery appears to be very well organised. In one case, it was found that 15 "tourists" had been organised in teams taking turns catching and processing the fish. The fish was then exported abroad in freezer vans or trailers, without the fish ever being declared.



# Criminal networks in business and industry

When criminal networks operate in business and industry, one or more members of the network are often linked to enterprises as facilitators, straw persons or partners. The networks invest money or provide human resources such as chair of the board, general manager or staff members, and they influence the decisions made by the enterprise.

More than 80 per cent of criminal networks examined by Europol use legal corporate structures to carry out their criminal activities.<sup>79</sup> The networks linked to employment and financial crime in Norway are traditionally characterised by multi-criminal activities committed in connection with legal enterprises or hidden behind business structures, from which they can acquire and wield market power and distort competition to displace legal businesses. Some criminal networks also profit from environmental crime. The networks often consist of career criminals, but the crimes committed become increasingly advanced and the persons involved have often known each other for many years.

There is often no clear distinction between networks involved in traditional organised crime such as drug trafficking, and networks engaged in financial crime or employer crime.

Enterprises are used as legal fronts to facilitate money laundering and benefit and loan fraud.

Such cooperation benefits both parties: actors engaging in employer and financial crime gain access to capacity and reputation for violence and capital in the form of cash and loansharking businesses. The criminal networks gain access to business operating and accounting expertise, as well as the opportunity to launder proceeds and earn a fictitious legitimate income which generates welfare benefits.

Combating criminal networks is necessary to safeguard our society, combat market distortions and the underground economy, and to maintain public trust. Confiscation is an important tool to prevent criminal networks from keeping their financial assets.

<sup>79</sup> Europol, "Serious and organised crime threat assessment (SOCTA)", 2021.



## Industries characterised by employment crime

In recent years, several new industries based on unskilled labour have emerged. This has enabled criminal actors to expand, take market shares and establish a presence in new markets. In many cases it is difficult for customers to distinguish between criminal and law-abiding actors, and the price is often decisive when selecting a supplier. Crime in business and industry has distorted competition and it is *likely* that legal businesses are being displaced in several industries.

The construction industry has for a long time been a hotbed of tax fraud and exploitation of workers. Many of the contractors offering house painting and carpentry services to private individuals work without declaring any income and most of the employees are unskilled immigrants from Eastern Europe.

The transport business is subject to few regulations and start-up costs are low. Criminal actors set up as sub-contractors, use sole proprietorships to avoid employer responsibility, and perform contract work for large transport businesses. They evade taxes and excise duties, launder their proceeds, do not declare their drivers' wages and subject them to unfair working conditions and social dumping.<sup>80</sup>

After the pandemic, some multi-criminal actors have established themselves in the restaurant industry by buying or taking over the operations of existing enterprises or establishing new ones. The actors use straw persons to conceal their links to the enterprises, engage in tax evasion, money laundering, violations of the Working Environment Act and use illegal labour. Some of these actors are also linked to drug trafficking. Most of the restaurant industry crime is linked to smaller restaurants and bars and fast food joints.

Various forms of work-related crime is also uncovered quite regularly in the car valeting and repair industries, with exploitation of foreign labour, undeclared wages and wage theft being rife.<sup>81</sup> Many foreign labourers work unregistered and temporarily in connection with the tyre change season. In some enterprises, there are indications that employees are being severely exploited. New regulations relating to the approval scheme for car valeting, wheel storage and changing will come into force on 1 July 2022 and may curtail opportunities for criminal actors.

<sup>80</sup> Økokrim, "Kriminelle aktører i varetransportbransjen", 2022.

<sup>81</sup> Politiet, "Arbeidslivskriminalitet i bilpleiebransjen i Oslo og Akershus", 2019.



Digitaler Galaxus AG

COOP

COOP

grill  
und kein  
Tosset!

Anbruch

SafeTouch  
Connect

112-C

MIB

NATURAL NATURE

1000

SafeTouch



## Professionals assisting criminals

Access to or the ability to influence professionals is often required to succeed with some forms of crime and avoid detection by the police and supervisory authorities. Proceeds of crime are concealed, camouflaged and laundered through the use of professional facilitators who make use of their expertise and the trust placed in them by society. It is *highly likely* that some professionals deliberately and actively facilitate crime.

Professionals such as lawyers, accountants, auditors and real-estate agents, as well as employees in banks, financial institutions and the health sector, have key roles in society, roles involving a high degree of trust. Due to their familiarity with rules and regulations, they also know how to circumvent them.<sup>82</sup> Although the percentage of professionals assisting criminals is small, the consequences are significant, as this undermines the trust in our societal model and the roles of these professions.

We have seen several examples of professionals assisting criminals with a wide range of services, using their roles to make a profit for themselves or others. In several cases, and across professions, there are close ties between the professionals and key actors in criminal networks. Several networks have access to professionals and corrupt employ-

ees in banking and finance, accounting and legal services. In some cases, professional actors themselves hold key roles in the criminal networks.<sup>83</sup>

Some lawyers are implicated in offences including leakage of classified documents and information, smuggling of goods to prison inmates and facilitation of abuse of client accounts, e.g. by evading the payment of debt to creditors or laundering proceeds of crime. There are also law firms which are probably owned by straw persons on behalf of persons convicted of serious crime and who are part of criminal networks.

Accountants are suitable facilitators of e.g. fictitious invoicing, tax evasion and accounting fraud to obtain loans on false grounds. There are accounting firms that have a significant proportion of known criminal actors within work-related crime on their customer list. A few accounting enterprises appear to exclusively offer their services to criminals.

Within banking and financial services, it is particularly assistance to obtain loans on false grounds that is provided to criminals. This kind of facilitation may constitute corruption when carried out by bank employees. In many cases, the relationship between the bank employee and the criminal is long-standing.

<sup>82</sup> Økokrim, "Temarapport – Profesjonelle aktører", 2021.

<sup>83</sup> Politiet, "Politiets Trusselvurdering 2022", 2022.



## Straw persons concealing criminals' links to enterprises

Straw persons are used by criminals to conceal the true owners of an enterprise, circumvent regulations, minimise detection risk and avoid prosecution. It is *likely* that the use of straw persons will increase due to the digitalisation of society and the opportunities for ID fraud.

There may be various reasons why criminals try to conceal true ownership, e.g. benefit fraud, circumvention of bans against running a business, having a criminal record or avoiding responsibility for the enterprise's criminal activities. The straw persons are often closely connected to the true owner(s) and manager of the enterprise, but they may also be victims of ID theft.

Actors in networks engaged in tax fraud and exploitation of workers are often mentioned in police intelligence databases in connection with various forms of crime, and may also have prior convictions and be disqualified by the court from operating businesses. To conceal that they in reality operate new enterprises, other persons are used as fronts in the formal roles of the enterprise. The same MO is seen among persons involved in serial bankruptcies. This enables them to win public tenders, as the certificates from public databases (eBevis) and the police presented with the tender relate to the straw persons and not the true owners and

managers.<sup>84</sup>

Criminal networks establish new sole proprietorships offering house painting and carpentry services every year and use them to defraud elderly citizens and commit employment crime when selling construction-related services to private individuals. Young female family members with no criminal record are often used as straw persons for male family members to lower detection risk and make the enterprises appear legitimate.

By establishing enterprises in other people's names, criminals can work undeclared and conceal undeclared incomes, while also receiving social benefits. In the transport industry, sole proprietorships are created in the name of foreign nationals who are victims of ID misuse or have lent their identities to others. The enterprises are used by criminals for their own businesses and to withdraw proceeds.

Identities can also be misused in connection with loan fraud, through enterprises being established in the names of people unaware of the fact. Fictitious reports of wages disbursed, employment etc. are also submitted for persons who were never employees of the enterprise. These fictitious reports form the grounds for loan applications submitted in the victims' names without their knowledge.

<sup>84</sup> eBevis and police certificates of conduct are submitted in public tenders to verify whether the supplier is bona fide or not, and whether there are reasons to reject the tender due to the provider having a criminal record or similar.



## Business structures used for moving and laundering money

Legal business structures are well suited for laundering proceeds of crime, as companies and enterprises generally have larger cash flows than private individuals, are afforded more credit and have a customer base to support the impression of a legal front.<sup>85</sup> It is *highly likely* that companies in industries that employ low-skilled workers will be used by actors involved in drugs and employer crime to launder criminal proceeds.

Money laundering through business structures mainly takes place by diverting the proceeds of crime to enterprises, or by laundering proceeds of crime through the enterprise.

Several enterprises in Norway are owned by or linked to actors well-known for drug trafficking. The enterprises are used to launder proceeds of crime and operate in industries with low-skilled workers and where undeclared wages disbursed in cash are common. Actors who evade taxes and exploit workers while also facilitating laundering of proceeds from drug trafficking, pose a particularly grave threat.

Some actors have roles in multiple enterprises and use the enterprises' bank accounts actively to launder money by diverting money to them and moving the money between accounts. Payments into these enterprises' accounts are often made by persons without assets or income, and who are known for various forms of crime.

Also more traditional forms of money laundering, e.g. conversion of proceeds into valuable objects, make use of legal business structures. Export businesses are often used for so-called trade-based money laundering, where legal goods are bought with the proceeds of crime.<sup>86</sup> The legal goods are then exported from Norway and sold abroad. Stockfish and fish heads have for example been paid for by proceeds from romance scams and then exported to Nigeria.

The laundered proceeds ensure a continued existence for criminal actors and networks.

<sup>85</sup> BRÅ, "Kriminell infiltration av företag", 2016.

<sup>86</sup> Financial Action Task Force (FATF), "Trade-based money laundering: Trends and development", 2020.





**ØKOKRIM**

**Postal address:** PO box 2096 Vika, NO-0125 Oslo

**Street address:** C.J. Hambros plass 2 C, NO-0164 Oslo

**Contact:** +47 23 29 10 00 / [post.okokrim@politiet.no](mailto:post.okokrim@politiet.no)

[www.okokrim.no](http://www.okokrim.no)