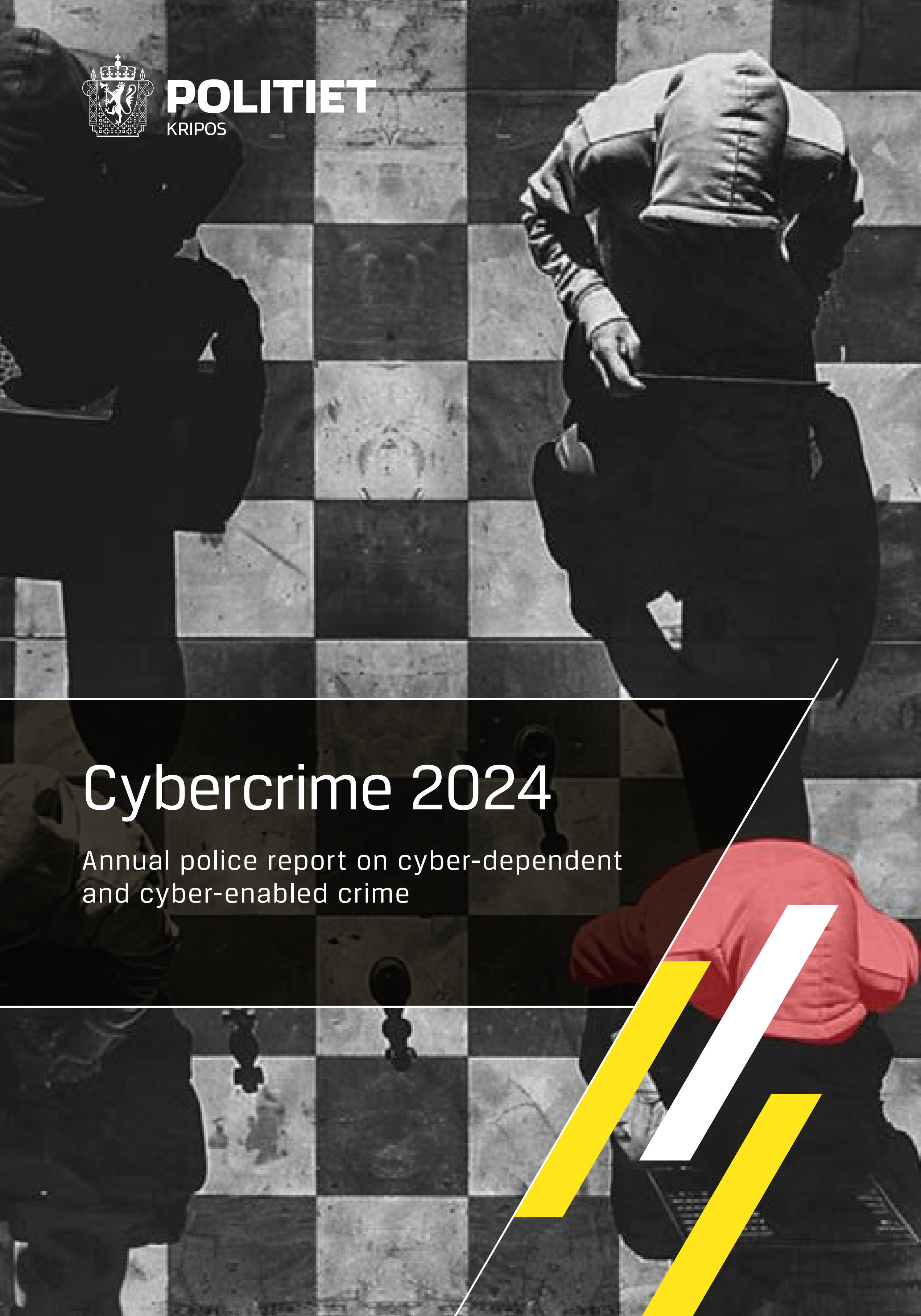
POLITIET
KRIPOS

Cybercrime 2024

Annual police report on cyber-dependent and cyber-enabled crime



Cybercrime 2024, NCIS
Annual police report on cyber-dependent and cyber-enabled crime

Layout: National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim)

Photo: Shutterstock

Preface

The threat landscape in cyberspace is becoming increasingly complex. Increased cooperation, specialisation and commercialisation of the crime, in addition to technological developments, drive cybercrime forward.

The extent of crime is large. Norwegian companies are attractive targets for criminals, but cybercrime also targets individuals. The threats are complex, and the tools and means used, are constantly evolving. Cybercrime was in 2023 spread widely across the country and the population.

The multifarious uses of information give cybercriminals more latitude and also increases their chances of success. The volume of stolen login credentials and data from compromised user accounts on illegal market places increased last year, illustrating the value of this information.

Cybercrime revolves around perpetrators with criminal intentions, global reach, and the will and ability to carry out a wide range of crimes. This will and ability must be countered by a combined effort from both the Norwegian private and public sectors.

Cybercrime 2024 provides a national situation report for cybercrime in Norway. The report was prepared by the National Criminal Investigation Service (NCIS) on behalf of the National Police Directorate. This is the second annual strategic intelligence report on cybercrime published by the NCIS.

With this report, the NCIS wishes to contribute with our knowledge of cybercrime, its targets and nature, using the terms we use in our daily work.

Kristin Kvigne
Director general of the NCIS

Photo: Shutterstock

Table of contents

Summary

There is no established universal definition of cybercrime.

In the report *Cybercrime 2023*[1], the NCIS defined cybercrime as the totality of two crime areas: cyber-dependent and cyber-enabled crime[2]. In this report, we have changed the Norwegian terms, but the translation in English remains the same.

Cybercrime has a broad impact, and increased in both volume and seriousness in 2023. However, national security mindset is maturing. It is clear that to cybercriminals, the value of information is increasing.

Both cybercriminals and the society that has to protect itself against cybercrime are evolving, and we see cooperation, specialisation and mutual dependencies increasing for both groups. Analyses show that both groups operate under the same parameters in cyberspace and use the same tools to achieve their goals. For cybercriminals it is particularly the commercialisation of crime, together with technological advances, that drive changes.

An important part of society's efforts to combat cybercrime consists of disrupting it. This report gives an account of the police's efforts in the past year. We also recognise that many other actors, e.g. public and private security organisations and product developers are constantly disrupting cybercriminal activity. This has a positive effect on combating cybercrime but it is also a driving force for criminal innovation. This will be a perpetual game of whac-a-mole.

In the preceding year, the NCIS had a particular focus on cybercriminal actors. Together with a focus on the combined threat from several crime types, this has resulted in better insight and understanding, which will be presented in this report. The similarity between how

[1] Report: NCIS, Cybercrime 2023, page 10, https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

[2] Described in IOCTA 2020, https://www.europol.europa.eu/cms/ sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

cybercriminals organise their activities and traditional hierarchical organisations, is striking. The presence of both inexperienced and specialised cybercriminals supports organised crime and is in itself an important driving force and recruitment factor for new crime. There are dependencies even between relatively autonomous cybercriminals like sex offenders. At the same time, it appears that the number of professional cybercriminals is far lower than previously believed.

The increased insight into the cybercriminal actor gallery has provided the NCIS with a number of new analytical tools. These are described in the report to establish a common terminology, form the basis for informed public debate and to increase society's ability to protect itself against cybercrime.

The report highlights what phenomena NCIS believe will have the most impact on the threat landscape, both current and long-term. Particularly, developments within cloud services and wireless lifestyle, ever more complex supply chains and the impact of artificial intelligence and cyberphysical systems, are highlighted as phenomena of critical importance to the situation in cyberspace on a tactical, operational and strategic level.

The report concludes that the best way to combat the complex and global threat of cybercrime is through joint cooperation and information sharing.

Purpose and organisation of the report

This is the second annual strategic intelligence report on cybercrime by NCIS. The purpose of these reports is to increase knowledge about cybercrime, both cyber-dependent and cyber-enabled crime. In this report, this will be done by describing the current threat landscape and the necessary conditions for and components of cybercrime, in addition to current trends. This report builds on the *Cybercrime 2023* report by further developing terminology and analytical tools, and by presenting updated threat assessments.

The source data on which the report is based, is mainly from 2022 and 2023. Norwegian sources are prioritised, and especially data from the criminal case register and the intelligence database. The source data is also based on information obtained from open sources and replies to requests for information sent to a selection of private and public sector partners.

The threat landscape 2023 (p. 10) provides an overview of cybercrime in the past year from the police perspective. The chapter focuses on key events and statistics of strategic importance to the development of the threat landscape.

The chapter on cybercrime (p. 21) gives a detailed presentation of the terminology used within the field. The chapter focuses on organised and other serious crime, and the account given illustrates the NCIS' mandate in cyberspace. The necessary conditions for cybercrime (p. 23) describe the components of cybercrime through analytical frameworks. The NCIS uses these frameworks to interpret and describe cybercriminal phenomena and trends, and the actors who commit the crimes. Based on the observations and experiences described in the chapter *The threat landscape 2023*, the chapters Cybercriminal approaches (p. 29) and Digital vulnerabilities (p. 49) introduce a selection of salient features of the cybercriminal ecosystem. The selection reflects key crime types and significant phenomena in the last year, and what developments the NCIS expect to see in 2024. These two chapters are meant for reference purposes where the subchapters can be read separately without further context or background knowledge. Trends (p.55) describe how the use of new technology and its adoption by cybercriminals', in the short and medium term, could influence cybercrime. Expected developments in 2024 (p. 75) summarises the strategic implications the threat landscape, together with various phenomena and trends in cybercrime, will have on Norwegian society, businesses and people. The assessments given in report are meant as decision support for preparation and implementation of countermeasures on various sociological levels.

The report uses a number of common terms that may have different meanings in other contexts. We have therefore prepared a glossary included at the end of the report to clarify the terms meaning in this report. Initial use of one of these terms in the text is marked by a key 🔑 symbol indicating that a definition can be found in the glossary.

The threat landscape 2023

Threats in cyberspace are shaped by a range of factors that exist in the analogue world. Interdisciplinary factors such as legal, economic, technological and political developments, societal change, individual circumstances and disruptions 🗝 influence the development of cybercrime. In the same way, these factors influence the police's ability to detect, prevent, investigate and prosecute cybercrime. The chapter presents the NCIS' view of the threat landscape in 2023 through an account of significant events 🗝 and overall statistics.

The NCIS observed a number of changes to the cybercriminal 🗝 threat landscape in 2023, particularly geopolitical and technological changes. The observed crime spread widely across the country and the population. Norway's many small and medium-sized businesses were particularly affected last year, although many individuals, large companies and municipalities also became victims of cybercrime.

Figure 1 illustrates observed developments in the crime types 🗝 monitored by the NCIS. The left shows cyber-dependent crime, which includes computer intrusion, data theft and cyber vandalism 🗝. The right illustrates cyber-enabled crime, which includes sexual offences, financial crime and organised crime. It is, for all practical purposes, possible to use computers to enable most crime types, but this account is limited to organised and other serious crime, e.g. sexual offences. The overall picture is pretty clear in that we have seen an increase in all types of crime with the exception of cyber vandalism, which remains stable.

However, the figures for cyber-dependent crimes are more uncertain than those for cyber-enabled crimes. One reason may be that fewer victims report cyber-dependent crime. Another reason may be that one type of crime is often commited in combination with another, and that in such cases it is the cyber-enabled crime that is recorded in the source data. The recorded numbers of online sexual offences against

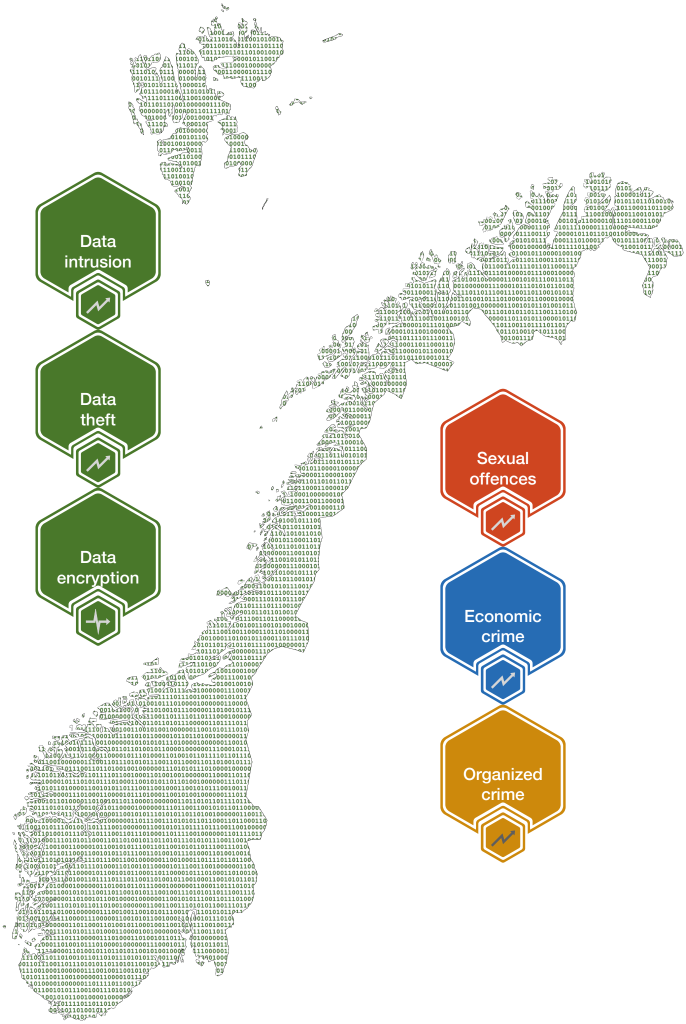


Figure 1: Trends in cybercrime monitored by the NCIS. The illustration was prepared by the NCIS

children ⊶, ⊶ are very uncertain. The NCIS is aware that many children never tell anyone about abuse they have been victims of online.

Cybercriminals are constantly developing and adapting techniques, methods, tools and strategies. They do this to become more efficient, pursue arising opportunities, increase profits ⊶ and evade countermeasures. The dynamics of cybercrime are reflected in the type of data which is in demand and traded on messaging services and criminal marketplaces. The use of criminal marketplaces confirms previous assessments that the majority of cyber-dependent crime is opportunistic and profit driven.

In recent years, cybercrime has moved

towards increased cooperation, specialisation and mutual dependencies. This contributes to the rise of a more closely interconnected cybercriminal ecosystem 🗝 making it easier for individuals with relevant skills and interests to partake in crime. This, in combination with a limited probability for criminal prosecution because of anonymisation tools and a decentralised economy, lowers the entry threshold for people to become involved in crime.

Cyber-dependent crime

Data theft continued to plague Norwegian businesses in 2023. Cybercriminals increasingly used information to carry out cyber-dependent crime, e.g. for social manipulation 🗝 and gaining access, or for extortion purposes. The various uses of information give cybercriminals more latitude and increase the chances of achieving their criminal aims 🗝.Globally, data theft doubled from 2022 to 2023.

The amount of stolen login credentials and data from compromised user accounts on illegal market places increased last year, thus illustrating the value of information in cybercrime.[3]

Despite the difficulties in tracing stolen personal data and business data to later criminal acts, we have a few examples of this in Norway. In 2023, several municipalities in Finnmark county became victims of computer intrusion. The perpetrators gained access through a compromised user account at a service provider. The investigation uncovered that the login details had been for sale on a criminal marketplace before the intrusion.

International statistics show that around 1/5 of all cyber-dependent crimes start at a third-party software provider 🗝. In 2022–2023, public sector organisations and digital service providers were the sectors most at risk. The intrusion cases in Finnmark were not the only cases in Norway in 2023 that can be characterised as supply chain 🗝 attacks.

There was a small decrease in the number of reported ransomware attacks in Norway last year, contrary to an increase internationally. Despite the decrease, ransomware attacks continued to be a major threat to national security with sometimes major consequences for Norwegian businesses. There were a few cases where denial-of-service attacks were used to extort victims 🗝, e.g. in combination with

[3] Report: Europol, IOCTA 2023, https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

a ransomware attack. Encryption of the victim's data remained an important tool in the cybercriminals' tool kit, with several new ransomware malware added in 2023.

Internationally, an increase is reported in ransomware actors who only steal data for extortion purposes rather than wholly or partially encrypting systems and networks. This is in line with the NCIS' observations of a few cybercriminal groups 🗝 and the widespread use of information in the commission of crime. Still, few examples of this were recorded in our systems, and the combination of data theft and encryption was still the primary approach 🗝 in 2023.

Much of cyber-dependent crime in 2023 illustrates the complex actor gallery and how a single crime can be driven by multiple motives 🗝 while at the same time having different value for different actors 🗝. For example, a number of Norwegian municipalities became victims of cybercrime in 2023, including attempted and successful computer intrusion, with and without subsequent encryption and ransomware attacks. Because Norwegian municipalities are responsible for and manage information about infrastructure and emergency preparedness, this information may have great intelligence value, even though the motives behind the attacks are unknown.

Fraud

Fraud attempts have become commonplace for most Norwegians and the sheer volume of sent fraud messages is now a shared problem in Norway and Europe. Phishing 🗝 was used in a series of different frauds, and fake websites were created faster than they could be taken down. The total fraud losses amounts up to billions of NOK and the number of victims increased. Over a million fraud attempts via telephone were stopped every month. The police recorded a total loss of NOK 287 million from online banking, investment and romance frauds in 2023.

Sexual motive

Cyber-enabled sexual offences differ in many ways from other cybercrime, inter alia in that sexual gratification is the dominant motive for this group of offenders 🗝. At the same time, of this crime is also profit-driven, and sex offenders develop new techniques and MOs just like other cybercriminals.

Norwegian cybercriminals committed a numerous sexually motivated offences in 2023, from involvement with child sexual abuse material (CSAM) 🗝 to cyber-enabled rape. In 2023 1230 offenders were reported in Norway for involvement with CSAM. The police received more than 13,500 tip-offs about offenders in Norway from the National Center for Missing and Exploited Children (NCMEC) and other collaborators.

Last year, an investigation was launched against a man living in Nordland county. He was later charged with sexual abuse of more than 250 Norwegian children in what is known as one of the largest child sexual abuse cases in Norwegian history ever. The abuse took place on Omegle[4], and the police found screen recordings of the abuse on his digital devices. The work to identify victims was still ongoing at the end of the year. The victims who had been identified were all between seven and thirteen years old at the time of the offence.

Omegle was shut down without warning in November. The site's founder declared in an open letter published online that Omegle had been used to commit crime and that the site had been met with criticism and resistance to such an extent that it was no longer possible to maintain operation of the site. There are still a number of similar sites but they have so far not been encountered as frequently in connection with sexual offences in Norway.

A common MO to establish contact with children online in 2023, was for perpetrators to pose as someone younger than their actual age. Other common approaches were to praise and compliment, appear friendly and trustworthy, and to offer money and other benefits, often in exchange for sexual services.

Other persuasion techniques were also used. Offenders behaved pushy or made threats, to induce children into sharing sexualised photos
and videos.

Children from the age of eleven shared sexualised material 🗝 with other children of the same age. Over the course of 2023, the material shared by children on social media became more graphic and extreme, in the form of increase in the number of rape and sexual

[4] Omegle was an American online platform and website that, among other things, was linked to indecent exposure and sexual exploitation of children online. Many criminal proceedings with Norwegian victims and offenders originated from the platform. The platform had an age limit of 18 years, but 13 years with permission and supervision of a parent or guardian.

intercourse videos. For example, a gang rape of a Norwegian girl was widely shared, by many children all over the country, Both boys and girls shared the video, and they mainly used Snapchat.

Reports of very young sex offenders increased in 2023, both of offenders under the ages of 18 and 15. Cases where the offender is under 15 years' old are not consistently reported to the police and are often handled without criminal proceedings. There will therefore be a number of unrecorded cases in this category. Most sexual offences committed by young people were cyber-enabled. The offenders were mainly boys, while the victims were mainly girls.

There has, in recent years, been an increase in adults who pay children for selfgenerated sexualised videos and photos. The sharing of photos and videos took place on social media platforms also in 2023, while payments were commonly made with direct payment apps, e.g. the Norwegian payment app Vipps. Although media files made up the majority of the content shared, there were cases where children streamed videos live to the offender.

The recorded cybercriminals who purchased sexualised material from children were men of all ages. The lowest reported age of children selling such material in 2023 was ten years. Some men bought material from multiple children, and some children sold material to a large number of men. The amounts ranged from ten to several thousand NOK. The majority of children who sold sexualised material were girls, but there were also a few boys.

The NCIS noted that many of the children who sold self-generated sexualised material had not been pressured, threatened or manipulated. The majority of children who fall into this category were motivated by money or recognition. Some children became victims of sexual extortion after having sold nude photos and videos of themselves. The offenders pressured the children into sending more sexualised content by threatening to publish previously provided photos and videos.

Offenders in Norway used cryptocurrency to purchase CSAM on the dark web 🗝 also in 2023. The identified offenders were mainly young men with IT skills. Only a few were were previously known sex offenders. In addition, dark web forums for sharing of CSAM collected funding in cryoptocurrencies to finance their operation. Other actors used a range of payment services to receive payment for CSAM, including money transfer services[5],

Politically motivated cybercriminals

On several occasions in 2023, Norway was targeted by politically motivated cybercriminals. As Norway play a key role in the West's support for Ukraine, both by sending military equipment for use on the front lines and through political processes in NATO, Norway has become a target for politically motivated hacktivism.

Norwegian businesses have in 2023 suffered down-time and loss of access to critical information as a result of denial-of-service attacks 🗝. Denial-of-service attacks may lead to businesses suffering reputation loss and loss of sales and services, but political interference and disruption of vital services and utilities has, so far, been limited in Norway.

Hacktivism is closely associated with denial-of-service attacks. Due to the limited damage they cause, the threat from hacktivists 🗝 has been down-played in Norway. The police are not aware of any denial-of-service attacks in 2023 that caused any serious technical damage or had any lasting consequences for Norwegian businesses. Some groups' warnings of future cyberattacks 🗝 that later fail to materialise, or cause less damage than expected, lead to less fear among the public and reduced media coverage.

Like other cybercriminals, hacktivists are not bound to a single approach or a fixed set of tools. At the same time, the membership of hacktivist groups is ever changing and a group's total capabilities 🗝 change through internal training, technological advances, available resources and membership fluctuations.

Law enforcement efforts

There are several actors and factors that play an important role in disrupting the cybercriminal ecosystem. This chapter gives an account of how police efforts in cyberspace have contributed to the disrupting of criminals' activites. In 2023, both Norwegian and foreign law enforcement have carried out several successful police actions 🗝 against cybercriminal networks 🗝 and individuals. After the actions, the police have observed that the criminal activity has moved to other platforms, and individu-

[5] E.g. Paypal and Western Union

als who escape arrest return with new tools and aliases. Although crime continues, these actions highlight police efforts to disrupt the cybercriminals' activities and demonstrate the police's ability to combat cybercrime through different methods. This work is time-consuming and requires international coordination and cooperation with other public and private sector businesses.

The police are in a unique position when it comes to investigating and prosecuting cybercriminals. This work gives the police unique insight into the criminals' plans, intentions 🗝 and motives 🗝, and supports investigations and preparation of preventive measures. Investigations have demonstrated that prosecution of key actors in cybercriminal networks have a far reaching and long-term impact on crime. Although cybercrime is multifaceted and complex, experiences show that basic human mechanisms also bring down cybercriminals.

This is why the police's efforts to prevent, investigate and prosecute crime committed in cyberspace 🗝 succeeded in creating disruptions in the cybercriminal ecosystem in 2023. In parallel with enforcing Norwegian law in cyberspace, the police prioritise prevention of sexual exploitation of children online and protecting businesses against cyberattacks.

Removal of CSAM from the internet

Last year, the NCIS succeeded in developing a new method for effectively hampering the sharing of CSAM on both the dark and clear web. Large quantities of CSAM are shared via commercial One Click Hosting (OCH) services[6]. The NCIS obtains passwords and links from various abuse forums, downloads the contents and verifies that the content is CSAM. The OCH service is then notified about the material and asked to remove it, with reference to the service's own guidelines.[7] The NCIS checks to see whether the service removes the material and notifies the domain reseller or domain registrar if it does not.

More than 20,000 links to CSAM have

[6] OCH services let users upload one or more files to a file sharing service where they can be shared with other internet users via a link.

[7] https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2023/09/25/ny-kripos-metode---vi-har-fjernet-titusenvis-av-filer-med-overgrepsmateriale/

been removed from the internet since the method was introduced. So far, around 90,000 videos and 1 million photos have been preserved as evidence. The NCIS plans to use artificial intelligence (AI) to find and identify children in the preserved material and to possibly remove them from ongoing abus.

An increasing number of Norwegian service providers want to follow foreign providers in cooperating with the police to report sexual abuse of children. In 2023, the Norwegian telecoms company Telenor signed an agreement with the police to detect and report CSAM on the company's cloud service "Min Sky". Telenor writes in its terms of use that CSAM and other sexualised material of children will be reported to the police and other relevant authorities and the user account closed without warning.

Hive

Norwegian and foreign law enforcement implemented a number of measures against cybercriminal networks in 2023. In January 2023, the FBI, the US Secret Service and Europol, with support from Norwegian police, took down the Hive network and service. Hive was implicated in a number of successful ransomware attacks against Norwegian businesses in 2021 and 2022. Hive was defined as ransomware as a service (see chapter 6.1). As a result of the takedown, Norwegian police have been able to study connections between Hive actors and other ransomware networks.

Developments in the Norsk Hydro case 2023 brought a breakthrough in the investigation of the 2019 intrusion into Norsk Hydro's computer network. Based on a European Arrest Warrant, an Armenian national who is suspected of being part of the cybercriminal group that attacked Norsk Hydro and a large number of other businesses in 2019, was arrested in Germany and surrendered to custody in Norway. The NCIS believes the man has played a key role in the group.

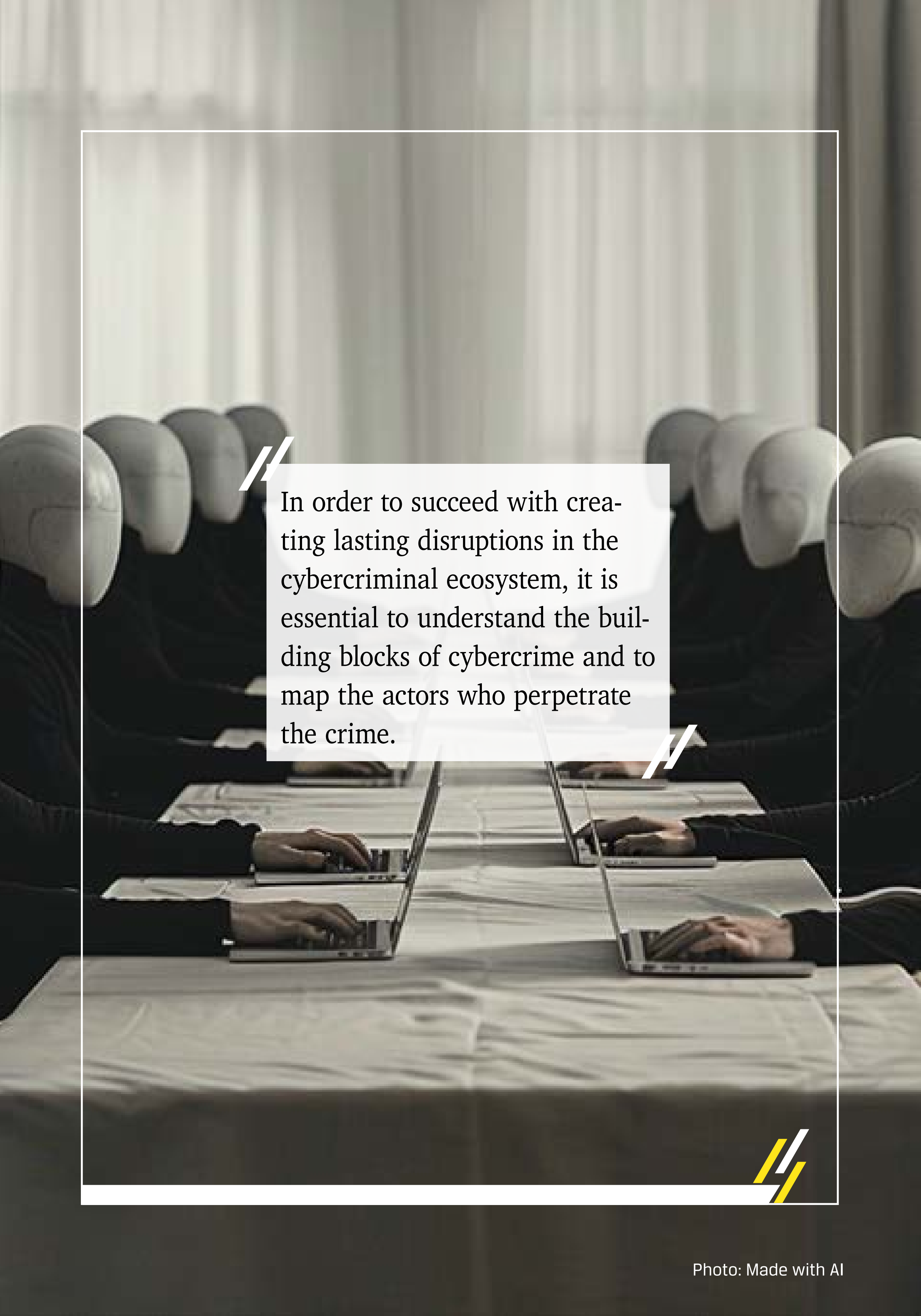
Towards the end of the year, officers from the NCIS were present when the

"Splash page" of the Hive platform after it was shut down.

Ukrainian police acted against the group. The action resulted in several persons being arrested, among them a leading figure in the group. The aim of the investigation is to prosecute the suspects in Ukraine, Switzerland, France and Norway.[8]

Ukrainian and Norwegian police in action in Ukraine Photo: The Police

[8] https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2023/11/26/kripos-flere-personer-i-kriminelt-nettverk-pagrepet/



In order to succeed with creating lasting disruptions in the cybercriminal ecosystem, it is essential to understand the building blocks of cybercrime and to map the actors who perpetrate the crime.

Photo: Made with AI

Cybercrime

Cybercrime is the sum of the two crime areas 🗝 cyber-dependent and cyber-enabled crime.

Cyber-dependent crime can only be committed in cyberspace and targets ICT[9] systems directly.

Figure 2 highlight the crime types cyber-dependent extortion 🗝 and cyber-dependent vandalism 🗝, which together make up the cyber-dependent crime discussed in this report. Several cybercriminal offences 🗝 can be committed within each of the two crime types, e.g. computer intrusion and data theft. None of these offences are exclusively tied to a single crime type. So far, the NCIS has no complete overview of all crime types and offences that can be

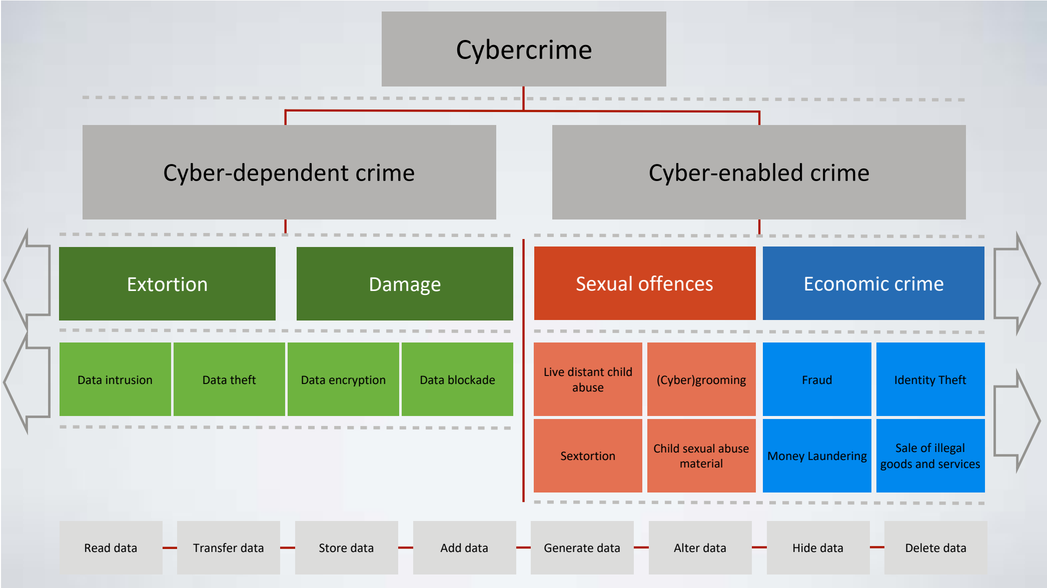


Figure 2: Categorisation of cybercrime. Model prepared by the NCIS.

[9] Information and communication technology

included in cyber-dependent crime.

Cyber-enabled crime is crime that existed before cyberspace but is enabled or made easier to commit with the help of ICT systems. This report is limited to discussion of sexual offences and financial crime. Contrary to cyber-dependent crime, where all approaches support both crime types, there are approaches specific to each of these crime types.

For example, possession of CSAM and sexual extortion are limited to sexual offences, while fraud and money laundering are limited to financial crime.

Particular to the field of cybercrime 🗝 is that there is a limited number of activities 🗝 that are enabled by the fundamental opportunities offered by ICT. At least one of these activities must be carried out to commit a cybercriminal offence. These activities are downloading, transferring and storing data, in addition to adding, changing, hiding, destroying and deleting data. The NCIS is not aware of other activities at the same conceptual level that can sustain cybercriminal offences.

Organised crime[10] affects all cyber-dependent crime discussed in this report plus some of the sexual offences and financial crime. There is cybercrime that is neither organised nor serious and therefore not illustrated in the model.

[10] Penal Code section 79c. Imposition of penalties exceeding the maximum penalty (multiple offences, repeated offences, organised crime)

Necessary conditions for cybercrime

In order to succeed with creating lasting disruptions in the cybercriminal ecosystem, it is essential to understand the building blocks of cybercrime and to map the actors who perpetrate the crime. The NCIS has for this purpose developed various frameworks that contribute to the understanding of the grasp connections between the actors, in addition to identifying key areas for preventing,

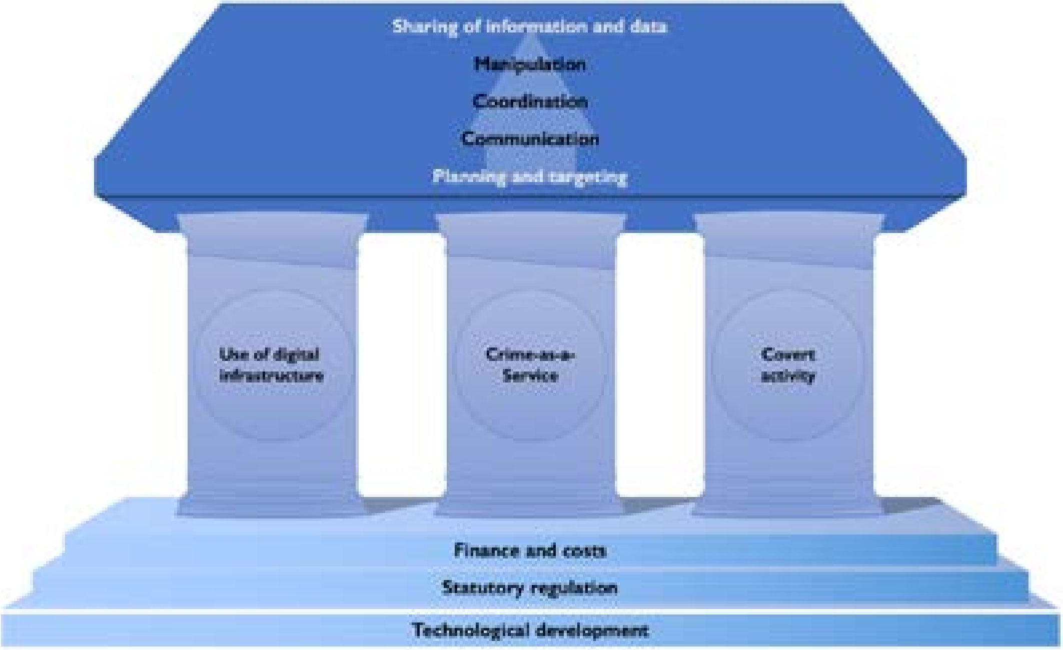


Figure 3: The eleven drivers of cybercrime. Model prepared by the NCIS.

averting and investigating their crimes. This chapter introduces the current frameworks used to help understand the necessary conditions for cybercrime.

Cross-sector drivers

From the police's point of view, the threat landscape in cyberspace is both complex and extensive. A framework can help to better understand the threat landscape and to be able to assess probable developments. The first steps were taken with the Cybercrime 2023[11] report, where the NCIS presented eleven cross-sector drivers of cybercrime. The three fundamental drivers: profit, legislation and technological development, are the most important in shaping changes in the threat landscape. This report expands on that analytical framework by describing the composition of the actors.

Criminal actors

Notwithstanding a complex threat landscape, criminal actors' motivations remain constant. This provides characteristics along which the actors can be categorised. Starting with assumed motivations, the NCIS has identified five basic roles:

- profit-motivated criminals
- sex offenders
- activists
- state actors
- terrorists

These five roles represent a set of motivations and intentions that are relatively stable and which lead to aims. An actor's aims can be specific or vague and can change over time. Aims are translated into plans which in turn lead to observable actions and activities. Methods and tools are continuously being amended and adapted to support the various actions taken by an actor. The actors' assignment to the different roles is domain independent[12] and, mostly, enduring.

Based on similar approaches, the police can establish profiles and ascribe them to actors. Different roles are often associated with a set of profiles based on approaches that naturally support an actor's intentions. Contrary to roles, which are mainly constant, profiles can be shifting, momentary or unchanged.

[11] Report: NCIS, Cybercrime 2023, page 14, https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

[12] This refers to the physical and digital domains.

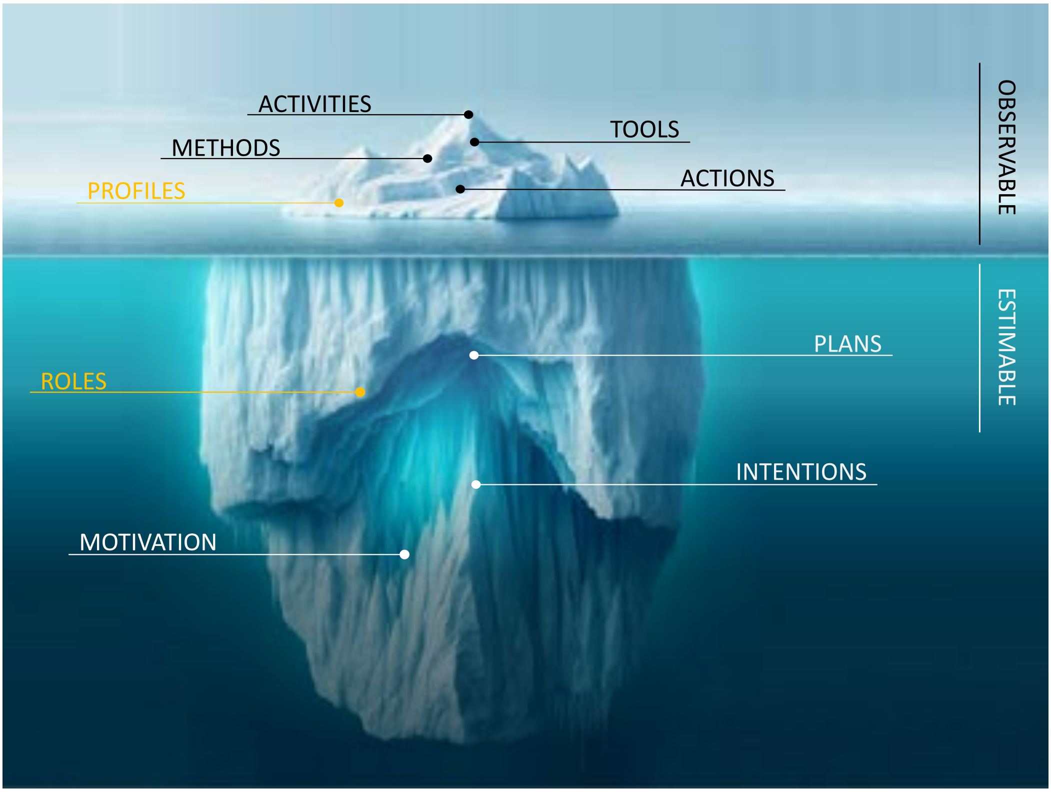


Figure 4: Composition of actors (text superimposed on an AI-generated photo). Model prepared by the NCIS.

This means that an actor can display several profiles at the same time. Examples of profiles are: malware developer, data thief, ransomware grouping, money launderer, fraudster and seller of live distant child sexual abuse.

Profiles are essential to understand the complexity of cybercrime. In addition to being key to the cybercrime service-market, the profiles' particular functions contribute to balancing the cybercriminal ecosystem. Neither roles nor profiles represent objective truths about an actor, but they are useful labels applicable to assess an actor's underlying motives and intentions.

Figure 4 illustrates to what degree the eight variables are visible or invisible to the police.

The importance of profiles to the cybercriminal ecosystem.
Because the criminals' approaches are constantly altered, the technical and tactical characteristics of different actors are also changing. The NCIS observe how some actors fit one distinct profile linked to the actor's presumed role. Other actors fit multiple profiles linked to the same role, while others fit profiles linked to different roles. The reason for the latter may, for example, be that an actor has multiple motives as a result of geopolitical circumstances, sexual preferences and desire for financial gain, or personal relationships and convictions. Another reason may be that an actor or a group of actors have a deliberate strategy of carrying out acts that pass under the authorities' threshold for implementing countermeasures. We have, for example, seen that state actors, directly and indirectly, use cybercriminals with different roles and profiles to carry out acts that support the state actors' intentions[13].

When actors are limited to cyberspace, consisting of a shared set of tools and methods that were never proprietary, the distinctions between the various types of cybercriminals and state actors are blurred. This in contrast to the analogue world, where the actors can be distinguished by many more identity markers and recognisable characteristics that make it harder for them to maintain operational security and deny involvement. In cyberspace, well-known techniques and methods previously used only by a few, can be shared with–or recreated–by others. This contributes to expansion of the shared cybercriminal toolkit and can lead to increased operational security and deniability among cybercriminal and state actors in cyberspace.

The possible ambiguity in the actors' underlying intentions, their ability to operate in secret a shared, digital toolkit and a common set of activities, lead to particular challenges with respect to investigation, prosecution and standards of proof in court. Without necessary context, actions seemingly in conflict with an actor's role can be interpreted as a deviation and from there lead to incorrect interpretations, hypotheses and assessments. For the police and other

[13] Often referred to as proxies

authorities this challenges their ability to coordinate and to handle cybercrime in grey areas ⊶. These challenges emphasise the need for better and increased information sharing and coordination across sectors and between public and privatesector organisations.

At the same time, the NCIS sees that many sexually motivated cybercriminals act independently and without the need for cooperation with others. Still, there are many actors in this group who collaborate with likeminded actors, not to avail themselves of their skills and knowledge, but to feel belonging and achieve sexual gratification by, e.g. sharing fantasies. Generally, sex offenders who wish to satisfy their sexual needs do not need to specialise or depend on others.

Like other cybercriminals, hacktivists are not bound to a single approach or a fixed set of tools.

Photo: Made with AI

Cybercriminal approaches

A reliable basis for decisiomaking requires a comprehensive understanding of the threat landscape. This requires knowledge of how intentions lead actors into actions, and how actors make us of technology to hide their identities, communication and cash flows. It is essential to draw a clear and detailed picture of the normal situation to be able to detect and identify indicators that can be monitored for rapid action and warning. This chapter therefore discusses a selection of cybercriminal approaches that have shaped developments in the threat landscape in 2023 and which the NCIS monitors to observe any change that influence developments in cybercrime.

Profit-motivated cyber-dependent crime

Cybercriminal actors need services in the form of specialised skills, digital tools and infrastructure, to operate their criminal business. This has created a market where digital services, tools and infrastructure are sold or rented out for criminal purposes. This business model is known as Crime-as-a-Service (CaaS) and has, over time, become the standard model in cyber-dependent crime.

The NCIS has observed that a number of cybercriminal actors with different roles and profiles depend on each other to carry out their crimes. Profit-motivated criminals make up one of the largest groups in the cybercriminal ecosystem.

Generally, CaaS can be described as an industry where cybercrime is commercialised and where networks of supporting services arise. This commercialisation distributes skills, tools and infrastructure in a way that makes crime available to everyone who wants to take part in it. IT skills and resources are no longer the most important barriers to enter into the world of crime, but rather own motivation and perceived prosect uion risk.

In Cybercrime 2023, the NCIS assessed CaaS to be an independent, cross-sector driver that would impact cybercrime on a strategic, operational and tactical level (see figure 3 on page 23). We have observed several instances of this in 2023.

We see that technological advances, e.g. the use of generative artificial intelligence (GAI) for criminal purposes, are quickly introduced on the criminal market. When cybercriminals adopt a new tool or service, others quickly follow, and the innovation can in a short time significantly boost cybercriminals' capabilities.

Risk owners 🗝 who protect digital assets try to come up with countermeasures to close vulnerabilities created by the innovation, resulting in what is often referred to as a game of whac-a-mole.

Many actors offer tools together with training, or their expertise through rental and subscription services for perpetration of cybercrime. Complete how-to manuals for e.g. computer intrusion, data theft and encryption, are sold on illegal marketplaces. It is expected that GAI will influence production of bespoke manuals to order.

We see an increase in both reverse engineering[14] and copying, in which threat actors 🗝 re-use tools that have proven effective. One trend we see is that cybercriminals assemble new ransomware from fragments of various stolen and leaked source codes.[15] The leaks of the Conti and LockBit[16] source codes are examples of how the source codes have been adopted by others to update and adapt existing malware, or to make new malware.

Cybercriminal groups

The most prominent example of CaaS is ransomware-as-a-service (RaaS). RaaS groups make up a large share of CaaS as it requires diversified skills, experience and resources to carry out a successful ransomware attack. This puts RaaS groups among the most important, play-

[14] A process through which ones tries to find out how something is made and works without any direct prior knowledge of its construction and functionality. This is done by testing and analyses. Also known as: Reverse Engineering. Store Norske Leksikon, https://snl.no/reverse_engineering

[15] Also known as: Franken-ransomware

[16] Two well-known RaaS groups which have targeted Norwegian businesses.

ers in the CaaS industry.

The NCIS has observed that many cybercriminals are involved in RaaS but that they contribute in varying degrees and that their skills differ. Some contribute with encryption of the victims' systems while others develop the malware.[17]

The NCIS has observed connections between cybercriminals involved with several pieces of ransomware at the same time. RaaS groups are dissolved and ransomware becomes obsolete, and are replaced with new groups and pieces of ransomware. The NCIS have observed how cybercriminals move back and forth between established and new groups, and their names turn up in several investigations. For this reason, the NCIS believes there are fewer key cybercriminals in the RaaS networks than previously thought.

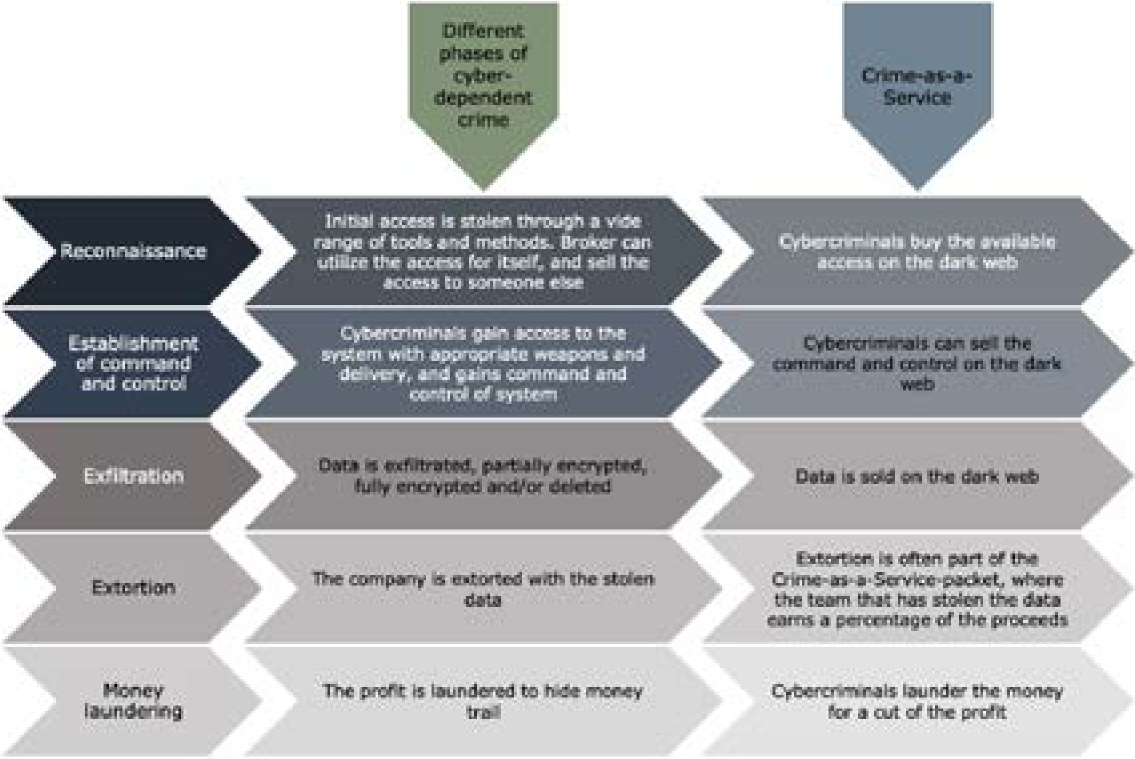
Cybercriminals have access to, and have used, many ransomware variants through the RaaS networks. The same infrastructure, e.g. servers used to attack businesses and store data, is used by multiple actors.

Profit opportunities in cyber-dependent crime

Criminals who commit cyber-dependent crime are particularly well served by CaaS because of the crime's complexity, required skills and multi-faceted kill chain 🗝.

The process of breaking into and interfering with a computer system 🗝 is made up of several illegal acts in interdependent phases. Data theft, for example, requires gaining access to a computer system, something which can be achieved in various ways. In the next phase, professional actors use stolen data to extort victims for profit. Figure 5 illustrates these phases. All phases can, to a greater or lesser extent, be purchased or rented on the CaaS market. In this way, a perpetrator of a ransomware attack can limit themself to organising and coordinating the attack and then purchase the necessary phases. There are also cybercriminals who offer to organise all phases in the cyber kill chain. In theory, criminals who wish to carry out a ransomware attack can limit themselves to describing the assignment and financing the criminal acts.

[17] Report: NCIS, Cybercrime 2023, https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf



	Different phases of cyber-dependent crime	Crime-as-a-Service
Reconnaissance	Initial access is stolen through a vide range of tools and methods. Broker can utilize the access for itself, and sell the access to someone else	Cybercriminals buy the available access on the dark web
Establishment of command and control	Cybercriminals gain access to the system with appropriate weapons and delivery, and gains command and control of system	Cybercriminals can sell the command and control on the dark web
Exfiltration	Data is exfiltrated, partially encrypted, fully encrypted and/or deleted	Data is sold on the dark web
Extortion	The company is extorted with the stolen data	Extortion is often part of the Crime-as-a-Service-packet, where the team that has stolen the data earns a percentage of the proceeds
Money laundering	The profit is laundered to hide money trail	Cybercriminals launder the money for a cut of the profit

Figure 5: Example of a selection of phases in cyber-dependent crime and associated profit opportunities. Model prepared by the NCIS inspired by the Cyber Kill Chain®

Recruitment and selection

Due to interdependencies, the transitory nature of cybercrime and the opportunities provided by CaaS, the cybercriminal ecosystem consists of multiple networks. Profit-motivated criminals and other actors cooperate both directly and indirectly in this ecosystem.

The NCIS has in 2023 seen how some of these networks are organised hierarchically along specific organisational patterns. This is not necessarily the standard, but there are similarities between groups involved in cyber-dependent crime.

Based on our observations, we divide the members of these networks into three categories based on skills and experience: inexperienced, specialised and organised cybercriminals.

Individuals are constantly being recruited to cybercrime and selected for each of these categories. The NCIS observes that what category a cybercriminal belongs to is decisive for the influence and benefits the person is offered. What

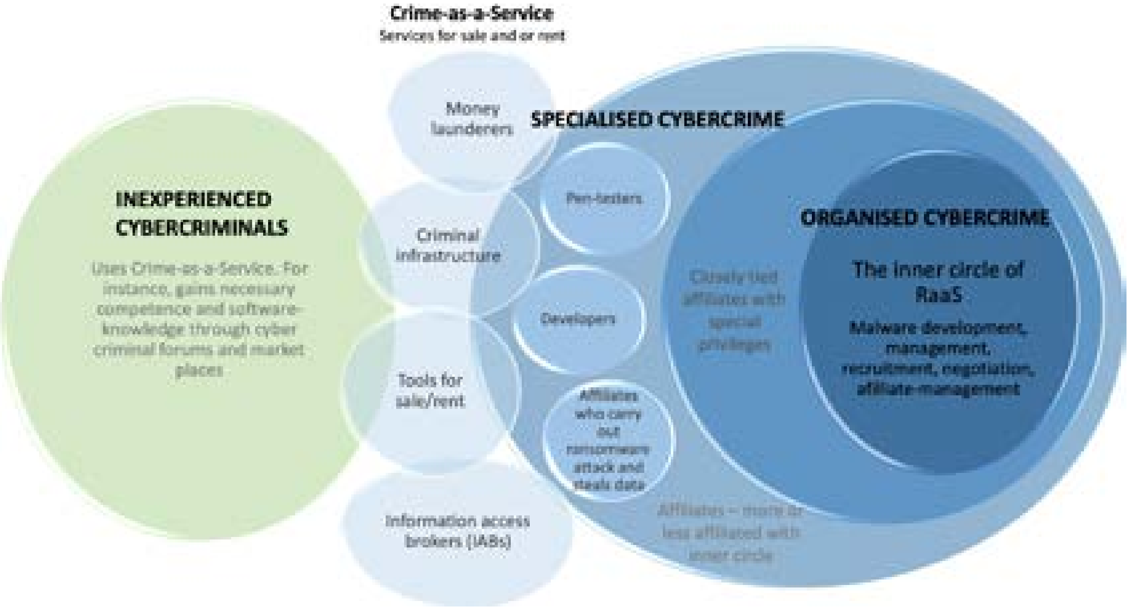

Crime-as-a-Service
Services for sale and or rent
Money launderers
Criminal infrastructure
Tools for sale/rent
Information access brokers (IABs)
INEXPERIENCED CYBERCRIMINALS
Uses Crime-as-a-Service. For instance, gains necessary competence and software-knowledge through cyber criminal forums and market places
SPECIALISED CYBERCRIME
Pen-testers
Developers
Affiliates who carry out ransomware attack and steals data
Affiliates – more or less affiliated with inner circle
Closely tied affiliates with special privileges
ORGANISED CYBERCRIME
The inner circle of RaaS
Malware development, management, recruitment, negotiation, affiliate-management

Figure 6: The various categories in the network demonstrating the gradual transition between the skills, activities and services on offer. Model prepared by the NCIS.

category a cybercriminal belongs to does not necessarily remain constant, they can move between categories. Their motives may differ, but most of the actors are driven by profit.

Inexperienced cybercriminals

It is easy for cybercriminals to purchase services on the CaaS market, something which makes the business model accessible to many more actors, including inexperienced criminals. The category inexperienced cybercriminals include, among others, the insider 🗝 and the "teenage hacker". Inexperienced cybercriminals may not have much technical skills, but they have sufficient motive and opportunity to commit cybercrime. Teenage hackers generally possess the basic technical skills required to acquire new and relevant knowledge, but they also possess a sufficiently strong interest to go searching for available source code, guides and manuals. Insiders already have an established access which, for example, can be used to harm the organisation or obtain an illicit gain.

The NCIS have observed that individuals without cybercriminal experience uses existing software available online to commit their first computer attack. They do not need any particular knowledge about the software and how it works. Finding such software is simple, and it is easy to acquire help from likeminded individuals online. The software is often free, and guides on how to launch an attack are easily available. Through their actions, inexperienced cybercriminals can be spotted and recruited by organised cybercriminals on relevant forums.

Specialised cybercriminals

Still, organised cybercriminal networks are often dependent on skilled and specialised cybercriminals who can take advantage of their services and earn money for their networks.

Specialised cybercriminals possess expert skills in their field, e.g. making malware or penetration testing, and often offer these skills on the CaaS market.

Specialists are commonly recruited from existing cybercriminal networks, often based on personal connections and reputation. We have seen how the networks cooperate, and how the specialists offer their services to several cybercriminal groups. If a network is taken down by the police, the specialists often resurface in a different network based on previous coorporation.

Organised cybercriminals use their presence and advertisements on cybercriminal forums and marketplaces to recruit specialists. This recruiting activity can be covert or discreet. It has even taken place openly in cases of broader searches. Closed channels on end-to-end encrypted messaging services like Telegram and TOX are also used.

The cybercriminals in this category are classified based on their expertise and experience. For example, it has been observed that initial access brokers 🗝 and money launderers play important roles in the criminal activities, but that they are often placed further to the left from the core (see figure 6) and have less influence in the group. They differ from specialists with technical skills, who are placed closer to the core group 🗝.

Organised cybercriminals

The organised level contains the members of the core group. The degree of organisation and collaboration is higher, and networks appear like ordinary hierarchical organisations with a senior management team giving instructions to the "staff".

It has been observed, for example, that RaaS groups operate with senior managers, recruitment officers and management of affiliates officers ⊶. The management team can, for example, be in charge of operations, develop malware and control negotiations with the aggrieved party. Members of the management team are considered highly professional cybercriminals, and a functioning management team is considered essential for durable RaaS malware. In the immediate circle around the core, we find affiliated cybercriminals of good standing and important specialists. They have varying authority and influence, e.g. they may be allowed to negotiate on their own or to recruit new specialists. Outside this circle are loosely connected affiliates who collaborate with the core group on a need's basis (see figure 6).

We have seen how various groups compete with each other for the most experienced and/or sought-after cybercriminals. In such cases we have observed how a larger share of the proceeds and more rights in the network are used for recruitment purposes.

Because organised cybercriminals need to manipulate people, services and equipment, both technical and language skills are in demand in serious cybercrime.There is also a demand for social skills, as manipulation of victims is considered a success factor.

There is a gradual transition between the two latter categories, the specialised and organised cybercriminals, where the most advanced activities are carried out by the organised cybercriminals. Inexperienced and specialised cybercriminals can also organise, but it is within the organised cybercriminals category that the organisation is professionalised.

Assessments

It is *likely* that CaaS is a self-reinforcing mechanism. As cybercriminals increasingly avail themselves of marketplaces to purchase skills and services, it is *likely* that their need to acquire these skills and resources themselves will decrease over time. This creates an increased demand for services, tools and infrastructure, which makes it attractive for criminals to offer their tools, services etc. on the market, something which in turn leads to increased specialisation of cybercrime. These developments have *likely* made cybercriminals more dependent on CaaS in the commission of their crime.

The trend is directing toward renting rather than owning. It is therefore *likely* that CaaS' importance as a driver of cybercrime increased in 2023.

CaaS is considered particularly important for the five operational drivers of cybercrime (see figure 3), where market developments influence the criminals' actions. The CaaS industry is itself influenced by the five drivers, as they form a framework for how the crimes can be perpetrated and there is a mutual dependency between the drivers for the cybercriminals to achieve their aims.

We expect that many more guides and manuals describing sub-processes in the cyber kill chain will become available. There is an *even chance* that these guides and manuals, over time, will reduce the demand for some services by providing inexperienced cybercriminals with the ability to commit serious cybercrime on their own by following the recipes in the manuals.

The NCIS observe how the same cybercriminals are members of several groups, that groups fragment or dissolve, but that the malware reappears under a new name. It is *likely* that there are fewer key actors in RaaS than previously believed. Although RaaS groups and networks are disrupted, it is *likely* that actors and skills move to other RaaS networks as a result of cross-collaboration. It is *likely* that collaboration is primarily transaction-based. It is *likely* that the actors are highly individualistic despite collaboration being essential for successful operations. Pragmatism is *highly likely* wide-spread in cybercriminal circles.

As cybercriminals are recruited from existing networks based on personal connections and reputation, and benefits in the form of a greater share of profits and influence in the group are granted based on skills and achievements, this will *likely* lead to cyber-dependent crime becoming more complex, as the ecosystem is driven by experience, and experience and expertise provide cybercriminals with new opportunities to acquire more experience and expertise.

Fraud

Social manipulation is commonly used in the commission of fraud, and well-known approaches are via email, telephone calls, texting and fake websites.

Social manipulation is about deceiving a victim into doing something that he/she otherwise would not want to. This is often combined with the cybercriminal impersonating someone to mislead the victim.

Despite interest rate and price increases, many Norwegians' have good finances. This makes Norwegians attractive targets of investment fraud and romance scams. The losses are often so massive that they have serious consequences for the victims' personal finances and family. This in turn, leads to significant non-financial difficulties.

The NCIS very often receive reports about investment fraud where the initial contact between victim and fraudster took place on dating apps. There is a connection between investment fraud and romance scams. It also happens that victims of romance scams are used as money mules 🗝. Commonly, the victims purchases gift vouchers with their own money and give them to the perpetrator, thereby laundering the money they have been defrauded of, or they buy gift vouchers with money deposited into their bank account and in that way make themselves guilty of handling proceeds of crime.

It has become clear that many of the cybercriminals encountered in fraud cases can be linked to organised and other serious crime. There are obvious similarities between frauds committed in Norway and Sweden, and which can also be linked to multinational drug and human trafficking gangs. The MOs are usually first observed in Sweden before they migrate to Norway. Examples are use of false documents, purchase of legitimate businesses and the use of fronts 🗝.

Many networks commit fraud by gaining access to victims' bank accounts through their login credentials, i.e. BankID in Norway. As for cyber-dependent criminal networks, the actors range from loosely associated networks with a core of fixed members, to organised networks with a hierarchy and line management in several countries. Based on information obtained from key actors it appears that the frauds themselves are committed by a small number of key perpetrators. One consistent finding is that key actors in BankID fraud to a large degree are also involved in drug trafficking and other types of fraud.

Assessments

It is *highly likely* that fraud will continue to increase and that persons of all ages and social classes will become victims of fraud in 2024.

Live distant child abuse

Live distant child abuse (LDCA) is live video of child abuse being streamed online to buyers who commission and pay for the abuse. The buyer can instruct the seller about how the abuse should be carried out. The rates are negotiated by the seller and the buyer, and payment is transferred to the seller through online payment solutions. Few technical skills are required to commit LDCA, and only basic English skills are necessary.

LDCA is sold by perpetrators in many countries on several continents, but an inordinate share of the crime is committed in the Philippines. The causes are likely complex, but the combination of a high proportion of English speakers, a well-developed internet infrastructure, poverty, certain cultural aspects and high availability of payment services have often been pointed out as significant.[18]

The recorded victims of LDCA are mostly girls of late primary school age who were abused by their parents, other relatives or neighbours. It is common for sellers to collaborate and, among other things, "swap" children for the purpose of abusing them, as well as to share chat service or payment solution accounts between them. As a consequence, LDCA is frequently an example of serious organised cybercrime.

The buyers of LDCA in Norway were all men. They came from all walks of society and few of them were recorded with sexual offences. Most of the men were single, and their average age was higher than the national average.

The NCIS considers that a significant share of LDCA buyers are situational abusers. Situational abusers have no basic intention of committing sexual abuse, but find themselves committing abuse when the opportunity arises. One example is a man who initially wanted to buy live-streamed adult sexual content, but who instead accepted the seller's offer of LDCA.

Assessments

Due to the fact that few of the offences are reported to the police, it is very hard to assess the scale of LDCA. The NCIS believes that between 400 and 2000 Norwegians purchased LDCA in 2023. It is l*ikely* that the number of sexual assaults committed by Norwegians is much higher than the number of perpetrators, as a perpetrator can commit many assaults in a year.

It is *likely* that the mental barrier preventing someone from committing rape online is lower than in real life, in addition to being practically easier. Reasons for this may be a greater degree of perceived anonymity online and that the physi-

[18] Report: International Justice Mission, Online Sexual Exploitation of Children in the Philippines, https://ijmstoragelive.blob.core.windows.net/ijmna/documents/Final_OSEC-Public-Summary_05_20_2020.pdf

cal distance to the criminal act makes it appear less serious.

Both technological development and the perpetrators' desire to minimise detection risk are important drivers for how crime will be committed in the years to come. It is *highly likely* that LDCA buyers will migrate to more secure platforms and payment services in the year to come.

Cryptocurrency

The NCIS saw in 2023 how cryptocurrency was used by all actors in the cybercriminal ecosystem across several crime areas.[19] Cryptocurrency was also used in innovative ways to conceal criminal acts, Use of cryptocurrency is no longer limited to cybercrime, it is now a component of all types of profit-motivated crime.

The NCIS has experienced that cybercriminals launder proceeds of crime through so-called mixing services, and mixing services run by cybercriminals are proliferating rapidly. Mixing services mix cryptocurrency flows to increase the owner's anonymity and to make cryptocurrency transactions harder to trace.

Mixing services are usually used in one of three ways. Either the cryptocurrency is forwarded to a central mixing service where control of the cryptocurrency is relinquished while the mixing process is ongoing. Alternatively, readily mixed cryptocurrency can be paid in return for a deposit with a mixing service. A third possibility is to retain control over own cryptocurrency while collaborating with others to mix the cryptocurrency between them. Although a mixing service can operate for some time, authorities are constantly working to find ways of tracing transactions, close services and prosecute the persons involved.

The NCIS has observed cases where cybercriminals have forwarded cryptocurrency to underground banking services. These services exchange the cryptocurrency to a particular cryptocurrency, usually a currency tied to US dollars to avoid exchange rate fluctuations, and store the money. The client then requests withdrawals in fiat money in a specific country, and can in this way launder illegal profits.

Cybercriminals use blockchain-based technologies like cryptocurrencies, which offer anonymisation, and which

[19] Particularly as means of payment in connection with the buying and selling of illegal goods and CSAM, laundering proceeds of crime, fraud and ransoms.

Cryptocurrencies are decentralised currencies outside government control. This independence offers anonymity at the cost of large short-term fluctuations in value.

Blockchains make it possible for two or more individuals, organisations or computers to exchange digital assets without knowing each other and without the involvement of a third party, e.g. a bank.

are therefore suitable for moving assets.

Theft of cryptocurrency has in recent years been a large and increasing problem globally. Cryptocurrency worth USD 3.8 billion was stolen in 2022, an increase from USD 3.3 billion the year before. Many of the large thefts of cryptocurrency were carried out via so-called decentralised financial services (DeFi[20]). These services store cryptocurrency and are particularly attractive targets for criminals. One example of a DeFi service is Bridges, which offers to transfer crypto-currency from one blockchain to another.

Assessments
It is *highly likely* that cybercriminals will continue to launder large amounts through the use of cryptocurrency.

It is *likely* that cybercriminal actors will use decentralised blockchains, cryptocurrencies and services with lax know-your-customer control and anonymisation functionalities. This makes it easier for criminals to move and launder criminal proceeds, also in Norway.

Proxy and VPN solutions

An often decisive factor in cybercrime is the ability to operate covertly[21]. Anonymisation technologies make this possible. The development of these techn-

[20] DeFi is an abbreviation of "decentralised finance" and is used as a catch-all for several different projects working outside the traditional finance system.

[21] In Cybercrime 2023 the NCIS identified "covert activities" as an independent driver of cybercrime. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

Cybercriminals want to put distance between themselves and the infrastructure used to commit crime. This is necessary to maintain their anonymity. The NCIS therefore believe that many choose to use commercial proxy and VPN services that store a minimum of information about its users rather than set up such solutions themselves, as this will make it difficult to create sufficient distance to the infrastructure. Also, setting up one's own proxy or VPN infrastructure is costly and time-consuming.

ologies is driven by legitimate privacy concerns and a desire for freedom in cyberspace, but they also benefit cybercriminals. As a result, the police face a constant challenge in managing the threat posed by criminals' use of anonymisation technologies.

Among other anonymisation technologies, proxy and VPN solutions 🗝 make up a substantial share of the tools used by cybercriminals. Cybercriminals use these technologies to hide their IP addresses and encrypt data traffic. This hampers detection and investigation of cybercrime.

Internationally, VPN was reported in 2023 as the anonymisation technology most commonly used by cybercriminals.[22] Europol also mentioned VPN as one of many encryption and anonymisation solutions frequently and increasingly used by sex offenders. During the same year, the NCIS observed that 40% of perpetrators who used file-sharing networks to upload and download CSAM, used VPN solutions. There were also examples of proxy servers being used as transit storage points for CSAM shared between file sharing networks Proxy and VPN solutions like Residential Proxy, Mobile Proxy and Residential Virtual Private Network cause particular problems. These solutions mask the users' IP addresses by using private individuals' internet subscriptions (IP address). It is difficult to uncover that these solutions have been used, something which in extreme cases may lead the police to investigate people for offences they haven't committed.

Ordinary proxy and VPN solutions can

[22] Report: Europol, IOCTA 2023, https://europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

be blocked from websites and online services through security measures designed to prevent criminal activity.[23] Cybercriminals can evade this problem by using Residential Proxy, Mobile Proxy or Residential VPN, which are hard for these security measures to detect. These solutions therefore have wider application beyond mere anonymisation.

Although it in theory is possible for the police to identify the end user of a proxy or VPN service, this requires the supply of the service being willing and able to disclose information about the end user. In practice, it is the NCIS' experience that this is seldom the case. Many commercial actors claim that they operate their services in a way that makes it impossible for them to disclose information about their users to the authorities. These actors present this as a guarantee that their solutions can safeguard the users' anonymity.

Overall, proxy and VPN solutions play an important role in the cybercriminals' ability to operate covertly. These technologies complicate an already complex ecosystem in which cybercriminals operate across borders and jurisdictions. This will be demanding for future crime fighting and the police will be forced to adapt their tools and methods to counter the constant development and spread of anonymisation technologies.

Assessments

Generally, proxy and VPN solutions reduce the speed of the users' data traffic. This may make it difficult to access and use certain online services. The NCIS believes that the slow speed of proxy and VPN solutions may drive cybercriminals to use other anonymisation technologies. The underlying infrastructure that supports the world wide web is gradually becoming better and the slow speed of proxy and VPN solutions will disappear over time. It is *likely* that this development will lead to increased use of proxy and VPN solutions by cybercriminals.

Commercial proxy and VPN solutions *highly likely* make it easier for cybercriminals with limited knowledge of operational security to operate anonymously on the internet.

[23] Examples of this are provided by some online banking services which use security measures to block commercial proxy and VPN services to protect their clients against fraudulent logins from suspect IP addresses.

End-to-end encrypted messaging platforms

Communication is a fundamental driver of cybercrime (figure 3), and cybercriminals are dependent on technology to communicate securely.

End-to-end encrypted messaging platforms 🗝 create numerous problems for the police. Messaging platforms increase the criminals' scope of action by automatic deletion of data and by protecting the information stored in the application with an extra layer of security. This makes it challenging for the police to access the information and important evidence may be lost. Like proxy and VPN services, the development of end-to-end encrypted messaging platforms is driven by legitimate privacy and security needs. For example, communication on Messenger became end-to-end encrypted in 2023 with the reasoning that it would provide the users with a more secure and private service.

End-to-end encrypted messaging platforms are easy to use, provides anonymity for cybercriminals, are stable, offer a good filesharing experience and low detection risk. The platforms are easily available and the user experience is the same as for other social media.

Cybercriminals differ in their motives and aims, and use of end-to-end endcrypted messaging platforms therefore has different value for different users. For sex offenders the technology offers

Telegram is a controversial end-to-end encrypted messaging platform. Telegram has been referred to as the "dark corner" of the clear web and has in recent years has seen a massive migration of cybercriminals from the dark web.

The criminal landscape on Telegram is multifaceted and complex. Guns, drugs and sex are sold on the platform, there is right-wing extremist content, radicalisation, hacking, fraud, sharing of CSAM and sexualised material of adults without consent, and exploitation of vulnerable people.

The NCIS' patrolling of Telegram has revealed that much of the crime takes place in the public groups and channels. From various sources NCIS has also learned that the more serious crime takes place in the private groups and channels.

> Child abuse is normalised on dark web forums and chat groups on end-to-end encrypted platforms. Such normalisation can lead persons who have not done it before to share CSAM or commit own abuse that they document.

Photo: Shutterstock

opportunity to perpetrate a range of sexual offences online, from conversations about sexual fantasies with others to live streaming of physical abuse of children.

Cybercriminals use the internet not only to commit crime but also to establish contact with and communicate with likeminded people. Child abuse is normalised on dark web forums and chat groups on end-to-end encrypted platforms. Such normalisation can lead to people without prior offences sharing CSAM or committing abuse and then documenting it.

End-to-end encrypted messaging platforms provide the opportunity to produce, download, store and share CSAM without there being an easy way to detect it. Sharing of CSAM requires online collaboration between sex offenders, but the degree of cooperation varies. End-to-end encrypted messaging platforms require little organising and administration. In comparison, sexual offenders on the dark web appear to be more organised as regards sharing of CSAM on chat sites and online forums.[24]

The NCIS has in the last year observed that sexual offences that were previously committed on open platforms have moved to end-to-end encrypted messaging platforms. Still, very few cases of sexualised contact between adults and children on such platforms have been observed. Such contact still takes place mainly on open platforms.

Assessments

End-to-end encrypted messaging platforms offer cybercriminals more elbow room. The technology offers both anonymisation and user friendliness, and covers the needs of both advanced and lowskilled actors. The platforms also provide a stable platform for exchange of criminal ideas. It is therefore *likely* that cybercriminals will increase their use of end-to-end encrypted messaging platforms in the years to come. This will challenge the police's ability to detect and investigate cybercrime on the platforms.

It is *highly likely* that Norwegian sex offenders will share self-generated CSAM and live-stream child sexual abuse that they themselves commit in one-to-one conversations on end-to-end encrypted-

[24] Report: NCIS, Cybercrime 2023, https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

messaging platforms. It is *likely* that sex offenders increasingly will transition to end-to-end encrypted messaging platforms as they are considered safer and provide a better filesharing experience.

It is *likely* that the scale of all types of sexual offences committed on end-to-end encrypted messaging platforms will increase in the years to come. Furthermore, it is *likely* that sexual offences that until now have been committed on other platforms, e.g. social media, will transition to encrypted platforms. It is therefore *likely* that contact between children and adults on end-to-end encrypted messaging platforms will increase in 2024.

Photo: Shutterstock

Photo: Shutterstock

Digital vulnerabilities

Like cybercriminals' actions, a discussion of digital vulnerabilities is necessary to draw a complete picture of the threat. Cybercrime must be combatted by society as a whole. Cloud services can contribute with security improvemens, because cloud service providers often have a bigger and more effective operation-, security- and development-environment. In this chapter, we wish to highlight a few vulnerabilities that the police believe are particularly important to increase awareness of and cooperation to combat cybercrime.

Cloud services

Businesses avail themselves of outsourcing services, including cloud services, as one way of gaining from technological advances and digitisation.[25] Cloud services can improve security in that the providers have large and efficient operation, security and development teams.[26] Cloud service providers will be able to update their systems faster, something which will benefit organisations that previously had to handle this themselves. In addition, cloud service providers will be able to handle updates of known and recently dicovered vulnerabilites much faster than organisations handling this themselves. Failing to update computer systems creates opportunities for cybercriminals.

Cloud storage makes rapid transfer of large quantities of data possible. We saw an example of this when Ukrainian authorities and businesses by using cloud technology were able to continue to support the population despite the mas-

[25] Report: NSM, Risk 2020, https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2020/skytjenester-og-tjenesteutsetting/

[26] Report: NSM, https://nsm.no/getfile.php/1313330-1696430485/NSM/Filer/Dokumenter/Rapporter/Nasjonal%20skytjeneste%20-%20konseptvalgutredning%20-%20KVU%202023.pdf

sive destruction caused by the war.[27]

However, cloud services also present challenges. Information and functionality are based on physical infrastructure located far away, often in other countries. Ownership structures and unauthorised access can be difficult to verify and control.[28] Cybercriminals can use this infrastructure to target businesses that have outsourced data storage, software applications and data systems to a cloud service. They can also use the cloud service provider's infrastructure to build systems and applications that the cybercriminals use in their operations. Cybercriminals avail themselves of legitimate services to upload large quantities of data to cloud services.

Norwegian and international law enforcement have for years seen how people with a sexual interest in children use commercial providers to share CSAM. This due to the low data transfer speed on the dark web making it unsuitable for file sharing. Instead, passwords and links to servers on the open web are shared on various forums on both the open and dark web.

A general trend is that businesses increasingly rent cloud services, and an assumption is that cybercriminals will follow this trend. If this assumption proves correct, cybercriminals will reduce their need to invest in hardware.

Zero-day vulnerabilities

Zero-day vulnerabilities 🗝 are hard to detect and the people who are able to find them often very competent. Historically, finding vulnerabilities in a piece of software that are unknown to the developer, has required specialised knowledge and expertise. Zero-day vulnerabilities can be sold for large

[27] Report: NSM, Nasjonalt digitalt risikobilde 2023, side 30, https://nsm.no/getfile.php/1313382-1697777843/NSM//Filer/Dokumenter/Rapporter/Nasjonalt%20digitalt%20risikobilde%202023.pdf

[28] https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2020/skytjenester-og-tjenesteutsetting/

amounts of money.[29] When a zero-day vulnerability is discovered, the owner must develop a security update 🗝 to close the vulnerability, which must be distributed to and installed on all vulnerable devices. Until the update is installed, it is possible for those who know about the zero-day vulnerability and have the skills to exploit it, to gain unauthorised access to a system. In 2023, zero-day vulnerabilities were found in software supplied by the developers Citrix and Cisco.

There have been several examples of criminal cases in which cybercriminals have exploited zero-day vulnerabilities to gain unauthorised access to computer systems. A Norwegian company became victim of a ransomware attack related to the Citrix zero-day vulnerability. The Norwegian branch of an American company was victim of computer intrusion with ensuing data theft by a criminal group in June 2023. A zero-day vulnerability was exploited to gain access. The profit-motivated group with ransomware as its MO is linked to Eastern Europe. It is uncertain whether the cybercriminal group found the zero-day vulnerability themselves or acquired the knowledge about the vulnerability from others.

In summer 2023, the computer systems of the Norwegian Government Security and Service Organisation were broken into with the help of a zero-day vulnerability. The matter was investigated by the regular police but was later transferred to the Police Security Service (PSS). The PSS decided to drop the case but attributed the attack to a professional criminal actor, probably a state actor 🗝.

Many companies are in the business of finding zero-day vulnerabilities. One of these companies[30] found 25 zero-day vulnerabilities in 2020, 69 in 2021, 41 in 2022 and, so far, 56 zero-day vulnerabilities in 2023. The trend has been rising since 2014.

Assessments

It is *likely* that malicious actors who succeed in finding zero-day vulnerabilities

[29] https://security.apple.com/bounty/categories/
https://zerodium.com/program.html
https://twitter.com/vxunderground/status/1562550443712352256/photo/3
https://www.wired.com/story/android-zero-day-more-than-ios-zerodium/

[30] Google Project Zero

are working on behalf of a state or are state-sponsored.

It is *likely* that it takes strong financial muscles to attract the expertise required to find zero-day vulnerabilities, and it is likely that only a few cybercriminal groups possess this capacity 🗝.

It is *likely* that the larger the proceeds of their crime, the more money cybercriminal groups have to attract actors with the right skills and knowledge to find zero-day vulnerabilities.

It is *likely* that technological weaknesses, e.g. zero-day vulnerabilities and other system independent vulnerabilities, will become more valuable to cybercriminals and increase the potential for damage as many businesses have the same weaknesses.

Even though they have a large damage potential, the NCIS believes that zero-day vulnerabilities are a lesser risk to Norwegian businesses than already known vulnerabilities.

Wireless lifestyle

Following the Covid pandemic, working from home has become common in many public and private-sector organisations. That the workplace has moved beyond the traditional framework has, however, given cybercriminals wider and more varied attack opportunities. The attack surfaces particularly increase in organisations that practice remote working on a large scale.

In addition to expanding them, the use of home offices has moved the attack surfaces beyond the organisations' traditional protective measures, e.g. firewalls and warning systems. This is problematic because people generally implement fewer protective measures on their internet access and digital devices in the home. Many people use weak passwords on their home wifi networks, do not use VPN or multifactor authentication, postpone important security updates and have multiple unsecured digital devices[31] connected to their networks. This brings with it an enhanced risk that employees will fall for the tactics and MOs cybercriminals apply to deceive and defraud.

As a result of these developments, employees have a larger responsibility in safeguarding the organisation's data security, particularly when staff work away

[31] "The internet of things" e.g. devices like robotic vacuum cleaners, stereos, smart TVs, etc.

from the organisation's premises.

The widespread use of smartphones has created new opportunities for cybercriminals who want to access sensitive and personal data. Fast and continuous internet access combined with an endless number of available apps and access points, make the smartphone an attractive target for malware developers. The possibility for users to install third-party software provides malware developers with new opportunities and functionalities.

Smartphones can be infected by malware in many ways. Malware can be sent via MMS or email, or it can be installed on a phone when attached to other compromised devices. The most common way of infecting a smartphone is, however, when the users themselves install third-party apps with malicious software. This most often occurs because the user is being deceived through various forms of social manipulation.

Many children have access to their parents' devices and online and social media accounts. This adds to the parents' vulnerabilities and constitutes an extra security risk for businesses.

When the NCIS examined the number of children under thirteen who shared sexualised videos of themselves online, one of the findings was that the youngest children often used their parents' accounts to share sexualised material of themselves. A large share of the tip-offs that the police received about sharing on YouTube, took place in the parents' names and with their user accounts. This was particularly the case for the youngest children (down to five years old) but the police also saw a few cases were the children were ten to eleven years old.[32]

[32] Report: Kripos, https://www.politiet.no/globalassets/dokumenter-strategier-og-horinger/kripos/seksuelle-overgrep/barn-under-13-ar-som-deler-seksualiserte-videoer.pdf

Photo: Shutterstock

Trends

As part of its crimefighting efforts, the NCIS tries to scan the horizon for trends that will change the criminal landscape. There are trends in society that we expect will have a future impact on cybercrime. In some areas the impact has already been noticeable for some time, while in others, the impact ihas yet to be observed. In this chapter, the NCIS will highlight the trends that we expect will have the greatest impact on cybercrime in the future.

Supply chain attacks

In an ever more globalised and digitised society, businesses make use of various third-party digital services and software. Costeffectiveness, focus on core business and increased productivity are reasons why business avail themselves of third-party suppliers and become part of a supply chain. This has its advantages, but also increase the risk of becoming victims of cybercrime.

Cybercriminals may exploit the poor security of a third-party supply of software and digital equipment. Malware can be embedded in software that is distributed to a number of customers and thereby give the perpetrator unauthorised access to the computer systems of one or more targets. Cybercriminals and other threat actors are constantly searching for the weakest link in the chain.

Public and private sector businesses in Norway are part of complex supply chains in which it is hard to monitor vulnerabilities. Businesses that operate

A supply chain attack takes place when a third-party is attacked but the real target is one or more businesses in the same chain.
Even though a business has implemented good physical and digital security, threat actors can exploit suppliers with poorer security to access their real targets.
Report: NSM, Risk 2023

fundamental national functions[33] are also part of these supply chains.[34] Fundamental national functions and/or ICT services that underpin them, can therefore become victims by being a part of a supply chain.

In January and February 2023, several municipalities in Finnmark county became victims of computer intrusion in connection with a supply chain attack. The investigation into the attacks has uncovered that the perpetrators managed to break in through a compromised user account at a shared third-party suppliers.

In principle, all businesses in Norway are potential targets of supply chain attacks. How vulnerable the businesses are, depends on how good control they have over purchases, logistics, security and dependencies. Legislation that places minimum security requirements on businesses will also influence this. In 2023 several attacks were observed where threat actors target third-party suppliers and software developers in order to attack their customers.

Assessments

It is *likely* that Norwegian businesses' different practices in how they organise and execute their purchasing, logistics and security, result in serious security challenges for vital services and utilities.

It is *likely* that introduction of new rules and regulations that will hold businesses responsible for complying with requirements for supply management and value chain risk will reduce cybercriminals' scope for exploiting vulnerabilities in supply chains.

Extortion in cyberspace

Criminals use extortion for financial gain. The means of coercion vary, but the aim is the same. Profit-motivated cybercriminals use both cyber-dependent and cyber-enabled crime to obtain these means, e.g. by getting a child to undress

[33] Fundamental national functions are services, production and other organisations whose business is of such national importance that disruption of the function will have consequences for the state's ability to safeguard national security interests.

[34] Report: NSM, Risiko 2023, https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

in front of a web camera, or by computer intrusion to steal information.

Sexual extortion for money

Since autumn 2022 the NCIS have noted a steady increase in sexual extortion with a financial motive. While previously mostly targeting grown men, the crime targeted ever younger boys. This trend continued in the first four months of 2023, also internationally.[35] During this period, the victims were boys aged 15 to 17, and the perpetrators organised,[36] unidentified actors operating from abroad, mainly Africa and Asia. Communication between perpetrators and victims was in English, and the perpetrators used false profiles pretending to be foreign girls until the victim had sent nude photos and/or videos of themselves. They then threatened to spread the images unless the victim paid. In several cases, the threats were carried out when the victim refused to pay, and in many cases payment was followed by demands for more payment. There have also been cases in other countries where the threats were directed at the victim's family after the victim took his or her own life.

Since spring 2023, the police have seen an increase in reports of financially motivated sexual extortion of victims in Norway. As before, the perpetrators were organised cybercriminal actors, but the amounts demanded were higher and the victims even younger, children down to 13 years old. In addition to the changes in victim profile, the cybercriminals changed their MO.

Many perpetrators made photo collages made up of photos received from the victim, photos found on social media and/or nudes of other persons, which they threatened to share. Text on the collages wrongfully stated that the victim was wanted for serious sexual offences against children urging recipients to spread the message virally, and text with identifying information about the victim.

Another change in MO is production of synthetic sexualised material of the

[35] https://www.fbi.gov/news/press-releases/international-law-enforcement-agencies-issue-joint-warning-about-global-financial-sextortion-crisis

[36] Report: NCIS, Sexual extortion of children and young people on the internet 2019, https://www.politiet.no/globalassets/tall-og-fakta/seksuelle-overgrep-mot-barn/seksuell-utnyttelse-av-barn-over-internett.pdf

victim. From other countries we received reports of artificial intelligence having been used to extort children, and in June the FBI warned the public that the technology can be used to generate sexualised images of children by using photos publicly available online.

Many of the victims, both children and adults, paid the perpetrators thousands of kroner due to the extortion. The amounts varied but were mostly in the NOK 5000–20,000 range, although we know of larger amounts being demanded and paid. In many cases, payment was demanded in crypto currency.

In late 2023, the police recorded cases of sexual extortion where the perpetrators used Norwegian names and language, possibly in order to appear more credible and/or to obtain the victim's trust before revealing his/her true agenda. The NCIS has yet to find out whether the perpetrators are the same organised networks using GAI to appear Norwegian, or whether they are Norwegians using a known MO to make money.

Sexual extortion places victims under exceptional mental and emotional strain, and they often feel guilt, fear and shame. We therefore believe that the number of victims of sexual extortion is far higher that the number of victims who report the crime to the police.

Assessments

Norwegian boys and men have paid large sums to extortionists. It is *highly likely* that extortionists consider Norwegians to be wealthy and able to pay, and that they will continue to target Norwegian boys and men in 2024.

The extortionists have demonstrated an ability to develop their MOs, which are becoming ever more cynical, inter alia by targeting younger boys and demanding larger amounts. It is *likely* that the extortion will have serious financial, psychological and emotional consequences for the victims. It is *likely* that a few of the victims in Norway will try to take their own lives as a result of extortion.

It is *likely* that cybercriminals will increase their use of GAI in financially motivated sexual extortion in 2024, and that the use of GAI will result in more children becoming victims of financially motivated sexual extortion.

Trends in ransomware extortion

The NCIS has observed how cybercriminals in some RaaS groups are adaptable and deliberate in their choice of which MOs and tactics are best suited to extort the individual victim. Normally, ransomware actors steal and encrypt data, followed by extortion. Targets can be picked at random or deliberately.

The information that is stolen, is often confidential or other sensitive information. They do this to put extra pressure on the victims to increase the probability of payment.

It has been noted that few Norwegian businesses pay ransoms to cybercriminals. In response, the measures the cybercriminals apply to obtain payment become more extreme. In 2023, the NCIS saw a change in the techniques some cybercriminal groups applied to extort Norwegian businesses.

This demonstrates how adaptable and dynamic the cybercriminals are. The NCIS has have, for example, seen cases of data theft through the use of ransomware, but without activating the encryption function. The data theft was followed by using the stolen data to extort the victims. Data theft without encryption changes the execution of ransomware attacks and suggests that information has become more valuable to cybercriminals.

Another trend The NCIS has observed, is that the perpetrators steal and then encrypt the data outside the victim's system, also known as remote encryption, followed by extortion with the stolen data as coercive means.

As an extra element in the extortion, the perpetrators have in 2023 also carried out denial-of-service attacks after having stolen data. The NCIS have also seen cases where the perpetrator has called the business to exert extra pressure. This is called triple extortion.

Also, the NCIS have seen that some ransomware actors publish stolen data online. This may increase the risk of repeated attacks against a business, as the stolen data is easily available online and can be downloaded fast, unlike downloads from the dark web.

The NCIS have received reports of ransomware actors contacting businesses saying that they have stolen data from their systems and submitting demands for ransom payments where subsequent examination of own systems find no indication of intrusion or theft. There may be may several reasons for this, which shows an interesting development worth noting.

Assessments

Lower willingness to pay among businesses who become victims of ransomware attacks will *highly likely* cause cybercriminals to find new and creative ways to continue extorting Norwegian businesses and increase their probability of success.

It is *likely* that a number of RaaS actors have increased their flexibility with respect to MOs and tactics to extract data and extort victims. There is an *even chance* that this is a result of better security awareness and culture in Norwegian businesses, including better backup routines and raised understanding of the value information has to the cybercriminals. Criminals' use of AI will simplify and automate the identification of valuable information in the victims' systems.

In cases where no sensitive information is missing and critical processes remain unharmed by a ransomware attack, better backup routines will *likely* reduce businesses' willingness to pay.

There is an *even chance* that ransomware built from leaked source code, in combination with the use of GAI, indicates that the perpetrators of ransomware attacks are inexperienced and lower-skilled cybercriminals. There is an *even chance* that these actors will adopt new MOs and extortion techniques to compensate for their lack of experience and knowledge.

Developments in RaaS will *likely* lead to a shift in the skills and tools needed to carry out ransomware attacks, from encryption and decryption to obtaining access.

It is *likely* that many RaaS groups have increased their knowledge of which targets are most vulnerable to attack and therefore the most profitable. Businesses that do not have or have not prioritised the resources needed to protect their assets, will be particularly vulnerable to attack. These are often small and medium-sized businesses.

Impact of artificial intelligence

Technological advances are a driver for change in the digital threat landscape. Despite artificial intelligence being in development for 60 years, it was only in 2023 that AI became a household word. The public debate has centred around the positive and negative effects of the technology on the one hand and sceptics who highlight its limitations on the other. The discussion tends to downplay the technology's present capabilities and its potential impact on future opportunities and threats. Developments in recent years and the public's general interest in AI constitute a force that drives technology companies, research institutes and the online community to new discoveries. This has led to political agreement between political parties and national governments about the need for stronger regulation.

AI capabilities

Despite the obvious limitations of current

AI systems 🗝, their criminal potential lies in the technology's speed, memory and almost limitless perseverance. In an imagined future where AI systems not only can compute but also understand,[37] the technology will change the threat of crime fundamentally. This is, however, only one of many future scenarios due to its immense potential. Despite the lively speculation about possible outcomes, it is important to assess the threat based on the technology in its current state.

Artificial intelligence can be applied in all crime areas and used to target individuals, organisations and states. AI improves and changes the commission of crime. The improvement is the result of automation, effectivisation and increased autonomy, while the changes mostly consist of quality improvements and resource optimisation. The result is an increase in the cybercriminals' capabilities and a potential for targeting victims at a large scale and high tempo with a large degree of customisation.

One of the most conspicuous examples of the use of AI is generative artificial intelligence (GAI). A sub-group of AI systems, GAI is trained on large datasets from various sources and can generate varied content based on foundation models 🗝 on request from the user. Since the introduction of ChatGPT in November 2022, the interest in foundation models has grown considerably, in parallel with developments towards increasingly multi-modal[38] functions. This development opens up for more complex interaction with foundation models and contributes to significantly reducing cost, time and skills required to commit some cybercriminal acts.

[37] AI makes use of statistical calculations and programmatic results through the identification of patterns in data. Despite the similarities between human and machine-generated content, the process for arriving at the end product is very different. To make an AI system understand in the same way as humans will require fundamental changes in how the technology works.

[38] Refers to AI systems that can receive, process and generate information across several different media (e.g. text, source code, image, audio or video). This means that foundation models can integrate and coordinate data from multiple sources.

Commercial versus open foundation models

The NCIS has previously considered open foundation models[39] to be a greater threat than proprietary, commercial foundation models[40]. Commercial models are the most advanced and have built-in censoring mechanisms to prevent misuse and undesired conduct. Although there are methods to circumvent these censoring mechanisms, the source code and datasets used to train the models remain inaccessible to the public. The risk increases considerably however, if the models' source code is leaked or published. This would allow users to remove the censoring mechanisms and adapt[41] the models for criminal purposes. Still, implementing, adapting, validating and maintaining foundation models of similar size and capabilities as the most advanced models requires considerable computing power and expertise, even when the source code is openly available.

Like other digital tools that automate and improve operations in the cybersecurity industry, foundation models have a dark side that can be exploited by cybercriminals. There are examples of models that have been developed and marketed for criminal uses. These include small, specialised models for specific tasks, e.g. password guessing, coding or speech and text generation for phishing campaigns. These narrow AI models are becoming leaner and require decreasingly fewer resources for development and use, and can operate independently of a third-party software provider.

AI agents

Like open foundation models, AI agents (AI 🔑) represent a considerable threat if used for criminal purposes. These agents are advanced problem solvers that adapt and react to complex, changing environments or received data. AI agents differ from foundation models in

[39] Used in this context to denote open source foundation models that can be downloaded and used without need for an internet connection or registering user accounts with a provider.

[40] Proprietary foundation models are models that are either free to subscription-based, but where the source code and training datasets are company secrets.

[41] Often called fine-tuning or re-training. Involves training already trained models on small datasets targeted for a specific purpose.

their ability to constantly draw conclusions and take autonomous action to achieve goals. AI agents solve multiple tasks simultaneously, adapt to changes in their environment and modify their actions to achieve a desired end state.

Current examples of AI agents are selfdriving cars and digital agents in portable devices and on the internet. Some of the tasks carried out by AI agents are monitoring of computers, web browsers and applications, and reading and writing of files[42]. They can also assign tasks to foundation models or collect data from human sources.

Applied to cybersecurity, AI agents have demonstrated considerable capacities through identification of threats and proactive implementation of dynamic security measures, something which may increase the effect of countermeasures considerably. The complexity of predicting the end state increases when intelligent agents which are programmed to prevent threats interact with agents with evil intentions. This can happen without human intervention or surveillance. This scenario can be applied to policing. The police want to use AI to investigate and prosecute criminals, while criminals want to use AI agents to avoid detection and prosecution. So far, the NCIS has not seen AI agents perform tasks in the commission of cybercrime.

Deepfakes are potent tools used to spread disinformation, deceive, generate sexualised content and coerce victims to do things they would otherwise not have done. Given the ability to create credible content combined with challenges in detecting synthetic text and media files, cybercriminals exploit the gap between rapid technological advan- ces and society's ability to adapt. Examples include cloning of voices for use in CEO fraud and extortion, or credible videos of politicians and public officials communicating fake information.

Criminal applications

Foundation models can generate content that in itself is illegal, e.g. incitement to violence or synthetic sexualised

[42] In this context, files may be digital information like software, text files, photos, music and other content that can be stored on a storage device.

The police may also be confronted with synthetic images that are so realistic that they cannot be distinguished from real CSAM, something which may lead the police to try to identify children that don't exist.

Photo: Made with AI

depictions of children. They can also be used in the commission of various cybercrimes,e.g. to generate text or speech for use in social manipulation or malware. Because foundation models represent a new potential vulnerability, cybercriminals can also attack the technology itself. This may lead to new MOs for digital extortion, data theft and cyber vandalism.[43]

GAI levels the playing field between actors in terms of skills and resources by making advanced and time-consuming operations accessible with fewer resources. One example of this is the dissemination of disinformation by troll factories 🗝, which falls outside current legislation.

The public, which must be able to trust the authenticity and origin of published information, find it increasingly hard to distinguish between true and false content. Through the use of GAI, criminal acts and activities which previously required considerable human and financial resources and therefore were associated with terrorist organisations and state actors, can now be perpetrated by a single actor with limited resources. The capabilities of groups and organisations with ample resources are thus scaled up correspondingly. This represents a potential for increasing the size, complexity, distribution and duration of disinformation campaigns. Without effective counter-measures, GAI may contribute to further reduce trust in information.[44]

Generative artificial intelligence in sexual offences

In 2023, the police observed several cases of AI being used to manipulate images of adults to produce fake nudes. The police also received the first reports of Norwegian perpetrators producing synthetic child sexual abuse material 🗝. Perpetrators wanting to use AI to gene-

[43] Successful exploitation of these vulnerabilities may offer large potential gain for relatively little risk. One concern is that personal identifiers and other sensitive information in the datasets that the models are trained on, may fall into the wrong hands.

[44] Report: NCIS, Generative artificial intelligence and cybercrime, https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/etterretningsrapport-generativ-kunstig-intelligens-kripos.pdf

rate CSAM discussed techniques and helped each other with advice on various darkweb forums.

Models that have been trained on adult pornographic material and models trained on non-sexualised photos and videos of children can be combined to produce synthetic sexual abuse material of prepubescent children, thus obviating the need to train the models on genuine CSAM. Nevertheless, perpetrators will train dedicated models on existing child sexual abuse material. This may lead to the children depicted in the synthetic material appearing to be real children, both children who have been abused sexually, and children who have not.

The police may also be confronted with synthetic images that are so realistic that they cannot be distinguished from real CSAM, something which may lead the police to try to identify children that do not exist. GAI can be used to mask genuine CSAM so that detection mechanisms will classify the material as synthetic. This may lead the police to not try to identify the depicted children because the material appears synthetic.

AI makes it easier for perpetrators to find arenas on the internet where there are children, plus acquire knowledge about how relevant gaming and communication platforms work. Furthermore, there are foundation models that apply deep learning to analyse and understand written text[45], thereby helping the user to adapt language, wording and expressions to make it easier for them to approach children online.

AI can be used to detect and prevent cybercriminals with a sexual interest in children from approaching them online. The police are working closely with the cybersecurity company AIBA, which has developed an AI tool that also can be used to detect and prevent cybergrooming[46] before the dialogue escalates to a punishable offence.

Assessments

Foundation models make activities like planning, reconnaissance and target selection easier to carry out and more effective. These circumstances, com-

[45] One example of such foundation models is: Large Language Models (LLM)

[46] Word borrowed from English. Defined as a process through which an adult contacts children (often by posing as another child) with the aim of committing sexual abuse.

bined with increased psychological distance to the victim through autonomous processes, will *highly likely* lead to an increase in the number of cybercriminals and their capabilities.

It is *likely* that the capability gap between cybercriminal and state actors will be reduced as a result of technological advances within artificial intelligence.

It is *highly likely* that cybercriminals' use of intelligent agents, taken in isolation, will end up becoming a larger threat than their use of foundation models. It is, however, *unlikely* that cybercriminals' use of AI agents will pose a significant threat in 2024.

Foundation models, procedures and datasets used to fine-tune AI systems for criminal purposes will *highly likely* be shared and sold on the clear and dark webs. It is *highly likely* that more and more advanced foundation models developed and designed for criminal purposes can be run on one single computer.

It is *highly likely* that GAI will be used to automate the creation and maintenance of massive numbers of digital profiles for fictitious persons and businesses. Over months and years, GAI will be able to carry out plausible activity through these profiles, thereby building plausible identities that can be used for various types of influencing and crime. It is *likely* that such identities will be traded as commodities.

Large datasets of sensitive and other valuable information will *highly likely* become attractive targets for data theft. These datasets can be used to train models or as input data to find connections that are hard for the unskilled to find. For example, it will be useful for cybercriminals to use GAI to obtain and collate relevant information from large databases such as public health registers, electoral rolls, population databases, scheduled trials and convictions, or registers of critical infrastructure.

It is *highly likely* that perpetrators will generate synthetic child sexual abuse images of children of all ages. It will be impossible to distinguish real from synthetic CSAM with the human eye.

It is *likely* that perpetrators will use AI tools to contact children on the internet, both to obtain knowledge about arenas that children use and to adapt language and jargon.

It is *unlikely* that new types of content of criminal use will be generated through the use of GAI.

A successful attack on industrial control systems could have immediate consequences for operational technology, the sur- roundings and human life.

Photo: Made with AI

The cyber-physical link

Cyber-physical systems

Until now, information technology (IT) has been viewed as an isolated domain with its own particular challenges, opportunities and dependencies. As the technology has advanced, human needs have driven developments towards increased integration of computer and network technology with physical processes. These are known as cyber-physical systems and include technologies we already use in our daily lives, e.g. assisted driving, the modern power grid and fast transport of goods.

This development has brought a number of benefits, e.g. more automated processes, simpler work flows and improved production, but also new dependencies and vulnerabilities that can be exploited by cybercriminals.

Modern industries depend on cyber-physical systems to a varying degree. Production, energy supply, shipping and the food and beverage industry are examples of this. These industries are often defined as fundamental national functions or are links in supply chains 🗝 fundamental to national security interests. The general trend in technological developments over the last 25 years has brought increased dependency on IT to produce, deliver and maintain goods and services.

Production and national infrastructure are not the only sectors that are dependent on cyber-physical systems. An increasing number of devices are produced which are designed to be linked to the internet and communicate with its surroundings. This concept is known as the internet of things and can be found in a range of consumer articles like household appliances, entertainment devices and health monitoring, in addition to administration of energy supply and climate control.

There are currently billions of devices that are linked to the internet. The number of devices has been growing steadily in recent years and they play an increasingly important role in our daily lives. In addition to making our daily lives, simpler, safer and more efficient, the internet of things also constitutes a growing vulnerability. A key concern is that as a general rule, these devices have not been designed with security in mind. This makes monitoring possible vulnerabilities and patching 🗝 them a challenging exercise. Increased dependency on technology, long and complex supply chains, a wide range of products and development driven by market demand rather than comprehensive security requirements, are important factors in making criminal exploitation of the technology a threat. In research projects, scientists have taken over control of selfdriven cars and exploited vulnerabilities in medical equipment[47], something which demonstrates the technology's potential for harm. It is important to have in mind that the potential for misuse is as great as the potential for legitimate use.

Threats to production industry Operational technology (OT 🗝) has for many years been subject to various types of disruptions from threat actors. Examples are disruptions resulting from ransomware attacks[48] or direct manipulation of physical processes through customised malware[49]. At a general level, the threat to production industry can be divided into two main categories: the threat against physical processes through cyber-dependent vandalism of OT and the threat against digital processes through cyber-dependent vandalism of IT.

In the context of cyber-dependent crime, direct manipulation of physical processes is often brought about by customised malware that targets the deepest layers[50] of an OT environment 🗝. The most important systems in an OT environment are industrial control systems (ICS 🗝), which gives threat actors the opportunity to manipulate hardware and computer communications involved in physical processes. A successful attack on industrial control systems could have immediate consequences for operational technology, the surroundings and human life. Experience has shown that development of customised malware for attacks on ICS requires highly specialised expertise, time and considerable resources, capabilities which so far have been limited to state actors. So far, we have only seen very few customised pieces of ICS malware "in the wild" 🗝.

Manipulation of digital processes involves a threat actor gaining access to a business' IT systems but without

[47] E.g. pacemakers, defibrillators and insulin pumps

[48] Example: Ransomware attacks against Norsk Hydro (2019) and Colonial Pipeline (2021)

[49] Example: Stuxnet (2010) and Industroyer2 (2022)

[50] OT environments are commonly divided into layers, from physical devices and equipment at the lowest level through control systems and monitoring functions to planning and management at the top levels.

necessarily gaining the opportunity to manipulate physical processes directly.

Such attacks will often have an indirect impact on the OT environment by making information inaccessible and preventing communication between systems and between systems and humans[51]. This will hamper the business' ability to maintain production and will in most cases have consequences for several links in the supply chain. Malware and other unauthorised access with the intention of harming the business' IT systems can in some cases also impact physical processes, either by the company itself shutting down production to limit damage, or by functionalities in the malware that makes it able to move between security zones in a computer network and manipulate ICS directly. Impact on physical processes can be unknown functionalities in a piece of malware, which generally have limited ability to manipulate ICS. Still, opportunistic malware attacks can have unforeseen consequences for physical production processes. But the most common consequences of manipulation of digital processes are on the businesses ability to produce and deliver goods and services, usually with wider consequences for the supply chain and society in general.

No OT environments are the same. The differences lie mostly in how the systems are composed and adapted to local needs. Direct manipulation of physical processes requires highly skilled expertise in both IT and OT, and thorough planning and reconnaissance. The cybercriminals' challenges in gaining access to protected industrial control systems combined with the high expertise required to exploit detailed knowledge about specific OT systems contribute to making manipulation of physical processes hard. Ransomware attacks therefore make up the majority of cyberattacks against production industry, and there are several examples of ransomware attacks having serious consequences for the company.[52] Even if physical processes are not harmed directly, a successful ransomware attack can lead to production stoppages and large costs. A recent example is the ransomware attack on Tomra in July 2023.

[51] Leads to the loss of the ability to monitor and control OT systems.

[52] Example: DP World Australia (2023), Colonial Pipeline (2021), JBS foods (2021), Maersk (2017)

Assessments

It is *likely* that OT-dependent businesses in Norway will become victims of ransomware attacks that impact their digital processes in the coming year. It is *highly likely* that Norwegian business and industry will be indirectly affected by cyberattacks abroad in 2024.

It is *likely* that OT-dependent businesses are particularly vulnerable to manipulation of digital processes as the willingness to pay increases with long supply chains and dependency on automation. It is *highly likely* that cybercriminal actors will continue to invent new extortion methods to make OT-dependent businesses more willing to pay.

There is an *even chance* that manipulation of digital processes in OT-dependent businesses will have unintended consequences on physical processes.

It is *highly likely* that the resources and expertise required to customise ICS-specific malware will be reduced as a result of developments in artificial intelligence, in combination with the source code of already known ICS-specific malware being publicly available. Due to the particularities and local adaptations of OT-systems, it will still be difficult to install and run ICS-specific malware.

As a result of digitisation and less resources and expertise being required to develop ICS-specific malware, there is an *even chance* that profit-motivated criminals will use ICS-specific malware to increase the pressure and willingness of industrial companies to pay during the coming three years. It is *likely* that awareness of the threshold for implementation of active countermeasures by the authorities will reduce the willingness of cybercriminals to target OT systems in organisations critical to society.

It is not obvious how profit-motivated criminals can financially benefit from physical manipulation as this type of attack generally leads to the systems being shut down, thereby leaving little room for negotiation. There is still an *even chance* that profit-motivated criminals will threaten to publish or sell critical vulnerabilities to other actors and in this way extort ransoms from businesses.

Expected developments in 2024

It is *likely* that the amount of cybercrime will increase in all types of crime in 2024. It is *highly likely* that cybercriminals will continue to invent new methods for realising their criminal aims based on geopolitical and technological developments, opportunism and newly discovered vulnerabilities. This will challenge the measures implemented to combat the crime. There is general need for better knowledge about and a disciplined cybersecurity culture on all levels in Norwegian society. More and better cooperation and information sharing between risk owners and the security communities are essential to forming a comprehensive understanding of the threat. It is likely that better cooperation will limit the damage caused by cybercrime.

Cybercrime has different impact at different levels of society, from fraud and sharing of sexualised material of minors at the individual level, new methods to force businesses to pay ransoms at the organisational level, to the need for international legislation and regulation of new technology which will impact society as a whole. The NCIS would like to emphasise the eleven drivers[53] of cybercrime, which are noticeable at all levels.

Threat to society

Cybercrime is a complex threat. It cuts across all sectors of society thereby posing a challenge to the Norwegian sector principle. This must be seen in connection

[53] Report: NCIS, Cybercrime 2023, page 14, https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

It is *highly likely* that cybercriminals will continue to invent new methods for realising their criminal aims based on geopolitical and technological developments, opportunism and newly discovered vulnerabilities. This will challenge the measures implemented to combat the crime.

Photo: Shutterstock

with the total defence concept and national emergency preparedness.

AI will *highly likely* challenge mutual trust in society by blurring the distinction between what is real and what is synthetically generated content. Increased mistrust can be exploited by all cybercriminal actors and be conducive for all criminal purposes in which human perception is a key element.

At the same time, it is *likely* that AI will challenge society's openness. The value of information increases with technological capabilities to make use of large amounts of data. It is for example *likely* that public registers available online will present new vulnerabilities that were not thought of when they were made available.

It is *likely* that the development with lower media coverage and public attention will force hacktivists to take new and more aggressive actions to achieve the desired effect.

The digitisation of society increases its vulnerability. It will be hard to monitor all vulnerabilities at all terminations in all businesses.

Digital security is increasingly becoming an individual responsibility. Increased technological dependency between businesses leads to a bigger potential for harm when one business' computer systems is compromised. It is *likely* that the majority of Norwegian businesses that become victims of computer intrusion in 2024 will do so because of a compromised business in the supply chain or via the services of a third-party software provider.

Vulnerabilities that cannot be patched, creative and opportunistic cybercriminals and malware traded online make OT-dependent businesses linked to fundamental national functions and critical infrastructure particularly attractive targets of cyberattacks.

Threat to businesses

AI will *highly likely i*ntroduce new vulnerabilities as businesses start using it, particularly in combination with better and more effective cybercrime.

Cloud services concentrate valuable information and are therefore attractive targets for profit-motivated criminals and state actors. This will *likely* make cybercriminals put more effort into breaking into the cloud services. It is *highly likely* that we will see hacking of and data theft from cloud services. There is an *even chance* that this type of computer breakins will increase the number of opportunistic targets for cybercriminals.

Cybercriminal groups will continue to become more professional, making them more capable and effective. There is *an even chance* that profit-motivated actors will become more attractive for other threat actors as a result of the trend towards professionalisation and in this way increase the value of crime as a service.

It is *likely* that ransomware groups will invent new methods for coercing victims. For example, cybercriminals can threaten to sell stolen business secrets to government enterprises to increase willingness to pay among the victims.

Threat to individuals

It is *likely* that AI will lead to more individuals inadvertently being harmed as a result of the automation and customisation of cybercrime. This will *most likely* be particularly true for fraud and disinformation campaigns.

It is *likely* that attempts to exploit individuals' remote access to critical business systems will increase as a result of our wireless lifestyle.

It is *likely* that more advanced and easily available anonymisation services will make it easier for cybercriminals to operate clandestinely.

Cyber-enabled sexual offences is a persistent hign threat. It is *likely* that the average age of both offenders and victims will be lower in 2024 than in the previous year. It is *highly likely* that the number of sexual offences on end-to-end encrypted messaging platforms will increase and it is *likely* that the use of these platforms will increase. It is *likely* that sex offenders will continue to develop their MOs in a more extreme direction, e.g. more aggressive persuasion techniques, and by application of AI.

Attachments

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

Probability terms

Assessments are always associated with some degree of uncertainty. To handle this uncertainty in a standardised and coherent manner, we have used probability levels (see table).

Terms and expressions

Glossary

⊶ **Cyberspace** is most commonly referred to as a global domain of interconnected computer systems and information resources and is also used as a metaphor, like the term "public space». This report uses cyberspace as a term for the totality of computer systems, networks, devices and software where cybercrime is committed.

⊶ **Computer systems** consist of one or more computers, pieces of software or other computer equipment that communicate in a digital ecosystem.

⊶ **The internet** is a global network of networks where smaller digital networks, systems and devices connect through a shared communication protocol. Cyber- crime occurs everywhere on the internet. That part of the internet we use for everyday activities is called the clear web.

⊶ **The deep web** is the sum of all unindexed content on the internet that is not immediately searchable with standard search engines. This is mostly comprised of legal content, such as access-controlled databases and paywall-restricted content. ⊶ **The dark web** is a small part of the internet consisting of networks with their own communication protocols. Navigating these networks

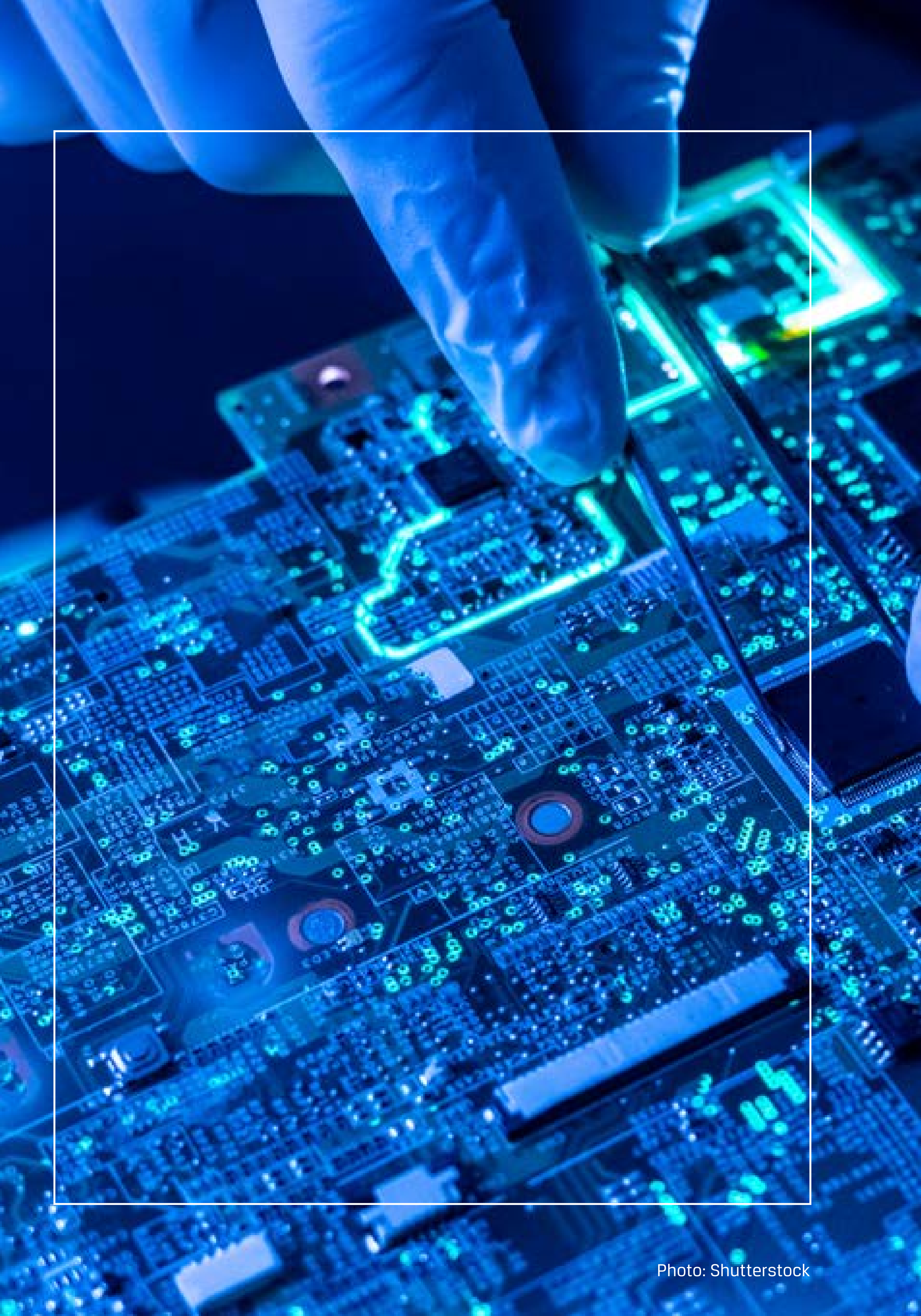


Photo: Shutterstock

requires specialised software.

🗝 **Crime field** is used in this context as an umbrella term which can include several crime areas within the same domain. 🗝 **Crime area** is used in this context to group related crime types. Cyber-dependent and cyber-enabled crime make up the two crime areas of cybercrime. 🗝 **Crime type** denotes the groups of offences on which registration in the criminal records database is based. In this report, the term includes cyber-related crime types such as computer crime and cyber vandalism. Other examples of crime types are sexual offences and financial crime.

🗝 **Capacities** refers to criminal's quantifiable physical, mental and digital skills and knowledge, while 🗝 capabilities require presence of both capacities and the ability to use them.

🗝 **Approach** is used to denote a particular course of action that cybercriminals generally use to achieve their goals,i.e. the methods and the sequences in which they are applied to commit criminal acts. Operational patterns and modus operandi are corresponding terms used in other contexts. Approaches combine 🗝 **cybercriminal** offences, e.g. computer intrusion and grooming of children, and 🗝 **activities**, e.g. changing, deleting or adding data.

🗝 **Event** is used in this report as a collective term for cybercrime, either cyber-dependent or cyber-enabled, and other activity in support of a military purpose. The Norwegian Penal Code does not necessarily include events, e.g. influencing operations[54].

🗝 **Cyberattack** is used in this report as a collective term for cyber-dependent crime such as computer intrusion and/or data theft and/or cyber vandalism. Cyberattack is also used about events that have not yet happened or that cannot be specified. In addition to being punishable under the Penal Code, cyberattacks also lean towards military purposes, e.g. sabotage, in this report denoted cyber vandalism.

🗝 **Grey areas** occur where areas overlap. The delimitation between various areas can be unclear for seve-

[54] The Norwegian Government has launched a proposal to criminalise harmful influencing operations. Press release: Regjeringen, https://www.regjeringen.no/no/aktuelt/regjeringen-vil-kriminalisere-skadelige-pavirkningsoperasjoner-i-norge/id3021665/.

ral reasons, and the area of overlap is denoted a grey area. Grey areas can occur anywhere. In this report, grey area denotes the grey area between state and cybercriminal actors, who, because they use the same tools, methods and activities, can be difficult to distinguish from each other. This challenges both jurisdiction and the police's mandate.

Troll factories are organisations and groups that use the internet to influence public opinion and political discussions, often through fake accounts and disinformation.

Social manipulation is a manipulation technique that exploits human weaknesses to gain access to private information, assets, etc. In English also Social Engineering.

Phishing is a word borrowed directly from English. It refers to methods for fraudulently obtaining other people's personal data and login credentials through social manipulation, e.g. through email.

Cyber-dependent extortion is in this report used to denote various cyber-directed MOs applied to extort a ransom from victims. It may be, but is not necessarily, limited to ransomware attacks. Other examples are threats to publish sensitive information or synthetically generated content.

Cyber-dependent vandalism is in this report used to denote cyber-dependent criminal acts and activities that damage ICT infrastructure and equipment without a discernible financial motive, e.g. denial-of-service (DDoS) attacks committed by hacktivists and sabotage of critical infrastructure.

Denial-of-service (DoS) attacks aim to prevent or damage access to a service, server or network. Eng: Denial-of-Service (DoS) Attack.

Cyber kill chain refers to a framework developed by Lockheed Martin to identify and prevent intrusion and malicious activity in a computer network. The framework describes the steps a threat actor must take to compromise a computer system. Eng: Cyber Kill Chain.

Disruptions is in this report used to denote the sum of all counter-measures implemented by the security industry (law-abiding individuals, scientific research institutions and public and private entities) which limit cybercriminals' scope of action. Disruptions can also be the result of actions and circumstances outside the control of the security industry, e.g. internal rivalisation between cybercriminal groups, geopolitical relations and physical damage to ICT equipment. These types of disruptions are not discussed in the report.

Police action is in this report used to denote arrests and searches and other interventions by the police to stop criminal activity.

⊶ **Cybercriminal ecosystem** constitutes the threat landscape where profit-motivated criminals, sex offenders, activists, state actors and terrorists operate, cooperate, collaborate, communicate, share, buy and sell, compete and collide.

⊶ **Cybercriminal networks** are constellations of individuals and/or groups who cooperate, are mutually dependent or exchange goods and services with the purpose of committing cybercrime.

⊶ **Cybercriminal groups** are collections of individuals who collaborate to achieve a common goal and/or commit cybercrime.

⊶ **Criminal and cybercriminal** are both terms used to denote persons who commit crime. Criminal is domain neutral, while cybercriminal refers to persons who commit crime in cyberspace. ⊶ **Offender and perpetrator** are used with the same meaning for variation purposes, particularly within the field of sexual offences.

⊶ **Motive** describes what actors wants to achieve through their criminal activity. Motives can be financial gain, sexual gratification, social change, access to sensitive information and perpetrating physical damage. An actor is described as motivated by pursuing a motive, e.g. financial gain. ⊶ Motivation refers to the fundamental driving force behind an actor's actions. Motivation is not only what an actor seeks to achieve, it is also the underlying reason why the actor wants to achieve this aim.

⊶ **Intention** is used in this report to denote the main, long-term state that actors put their efforts into achieving. Intention is not only the sum total of concrete plans and goals, it also describes a desired end state.

⊶ **Profits and financial gain** are used interchangeably as catch-all terms to describe criminal profits and earnings.

⊶ **Actor** is a collective term encompassing both individuals and groups. Group is for example used for specific groupings that commit ransomware attacks and are described as "ransomware actors". ⊶ **Threat actor** is used as a variation of the term actor and includes state actors, some cybercriminals and cybercriminal groups who constitute a specific threat.

⊶ **State actors** are nation states which constitute a threat or who commit cybercrime.

⊶ **Hacktivist** is an actor (individual or group) who commits criminal acts in cyberspace to promote a religious, political or other ideological message. The term must not be confused with "activist" which is both domain independent and does not indicate any criminal activity.

🗝 **Insider** is a current or former employee, consultant or contractor who has or has had legitimate access to the organisation's information systems and who misuses their knowledge and access to commit acts that causes harm or financial loss to the organisation[55].

🗝 **Money mules** are individuals who reluctantly, willingly or through persuasion place their bank accounts at disposal as an intermediary in a money transfer or who purchases gift cards and send them to their taskmasters. Eng: Mule.

🗝 **Front** refers to someone who acts as a front for someone else for the purpose of concealing the true ownership behind a transaction or asset. Fronts give individuals latitude to commit crime by making them "invisible" to public authorities

🗝 **Core group** is the term used for the inner circle of cybercriminals in a RaaS system. Depending on context, "RaaS group" is also used to denote the core group.

🗝 **Affiliates** are persons who have a business relationship with a ransomware-as-a-service core group and who avail themselves of the service. Eng: Affiliates.

🗝 **Initial access broker (IAB)** is used to denote cybercriminals who steal and/or sell stolen information and illegal access to computer systems. IAB is an example of a profile often associated with the role "profit-motivated criminal". Eng: Initial Access Broker (IAB).

🗝 **Supply chain** includes all links in the chain of supplys and sub-supplys who produce or supply goods, services and other factor inputs necessary in a business' delivery of goods or services from raw materials to the finished product.[56] Supply chain is in this report used to denote the sum of supply chain and the internal processes applied in a business to deliver goods or services to the next link in the supply chain.

🗝 **Third-party software providers** are owners/supplys of products or services used by others.

🗝 **Zero-day vulnerability i**s a security hole in a software unknown to the

[55] Report: NSM, Innsiderisiko, https://nsm.no/getfile.php/133153-1591706148/NSM/Filer/Dokumenter/Rapporter/Temarapport%20innsidere.pdf

[56] Report: NSM, Risiko 2023, https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

developer and discovered by attackers first.[57]

🗝 **Security update i**s the process of installing updates to software and systems. 🗝 Patching involves closing security risks, repairing flaws, improving functionality or improving a system's protection against cyberattacks. Eng: Patching.

🗝 **"In the wild"** refers to a genuine threat (i.e. not just theoretical) that can potentially harm computer systems and has been observed in cyberspace. The term is often used to denote newly discovered malware or zero-day vulnerabilities outside a controlled test environment. Eng: In the Wild.

🗝 **Proxy services a**re networks of multiple servers that function as intermediaries (nodes) between internet users and the internet. When an internet user uses a proxy service, the user's IP address is hidden behind the proxy node's IP address. The destination website (internet server) which is the target of the user's internet traffic, will then be unable to record/log the user's true IP-address. 🗝 **VPN services** use the same network structure and adds another layer of security by encrypting the traffic between the user and the nodes of the VPN service. It is the encryption that distinguishes a proxy network from a VPN service. In this report, proxy networks and virtual private networks (VPN) are denoted "solution" or "service". "Solution" is used where proxy networks and VPN are discussed together, while "service" refers to solutions operated by a commercial actor.

🗝 **End-to-end encrypted messaging platforms** use end-to-end encryption. This means that only the participants in a closed group can access messages sent between them. The messages and the files are encrypted with a key that is only shared between the sender and the recipient before they are sent over the network. Audio and video messages can also be encrypted with end-to-end encryption.

🗝 **AI system** is a collective term for various soft- and hardware that carries out instructions, physically or digitally, based on interpretation and processing of structured and unstructured data for

[57] Report: NSM, https://nsm.no/getfile.php/1313382-1697777843/NSM/Filer/Dokumenter/Rapporter/Nasjonalt%20digitalt%20risikobilde%202023.pdf

the purpose of achieving a given aim.[58]

🗝 **Foundation model** is an AI system that can be adapted to a range of different tasks, e.g. language translation, photo and sound analysis, in addition to generative abilities. These models are the foundation of a number of AI applications, e.g. OpenAI: ChatGPT, Google: Gemini and Midjourney. Eng: Foundation Models.

🗝 **AI agents** can be described as a team of automated robots characterised by high efficiency, endurance and the ability to find optimal solutions to a problem. Key functionalities include interactivity, flexibility, reactivity and proactivity. Eng: AI Agents eller Intelligent Agents (IA).

🗝 **Operational technology (OT)** is the part of cyber-physical systems which involves physical processes, often used in industrial production and other large-scale physical processes that use computer and network technology. Eng: Operational Technology (OT).

🗝 **Industrial control system (ICS)** is in this report used as a collective term for devices, protocols and sensors that interact in an OT system. Eng: Industrial Control Systems (ICS). 🗝 **OT system** refers to both physical and digital systems used to operate, monitor, control and secure industrial operations and physical processes.

🗝 **Victim** is used to denote anyone who has been a victim of a crime or unwanted interference. 🗝 **Risk owner** is used about businesses that risk becoming victims of crime. Sometimes, risk owner is also described as a 🗝 **target** of crime.

🗝 **Child** is in this report a person under the age of 18. Boy and girl are used when a child's sex is specified. A distinction is made for offenders who are under 15 years old, as they are under the age of criminal responsibility[59].

🗝 **Child sexual abuse material** or 🗝 **material depicting sexual abuse** of children are depictions of sexual abuse of children or depictions that sexualise children under 18.[60] 🗝 **Synthetic child sexual abuse material** is used as a collective term for all material (images, video, text etc.) that contain sexual abuse of children or in other ways sexualise

[58] https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/no/pdfs/ki-strategi.pdf

[59] Penal Code section 20, subs. 1a)

[60] Penal Code chapter 16, section 311

children, and that are made with generative artificial intelligence.

The eleven drivers of cybercrime

Technological development: Technological advances are made at breath-taking speeds and are constantly providing new opportunities and challenges for cybercriminal activity.

Statutory regulation: Laws and regulations open and limit the scope of action for both cybercriminal actors and law enforcement. Legislators are always behind.

Finance and costs: The digital economy makes it possible to carry out financial transactions without regulation and creates new opportunities for making a profit.

Covert activities and anonymisation technologies: Advanced anonymisation technologies make it easy to act without or with a false identity, simplifying an actor's ability to act covertly.

Crime as a service (CaaS): Buying and selling of criminal services, software and other products help make crime more profitable, finance new crime and make it easier for actors to commit crime that they would otherwise be unable to commit.

Use of digital infrastructure: Easy access to digital infrastructure through purchase, hire or theft makes it easy to obtain the digital infrastructure necessary to sustain criminal activity at low cost.

Planning and deliberate targeting: Easily available information in cyberspace and powerful hardware equipped with suitable software make planning and facilitation easy for both opportunistic and targeted actors

Communication: Hardware linked through the internet's communication protocols gives perpetrators' global reach and the ability to communicate with text, speech, video and data.

Coordination: Ease of communication eases coordination between multiple actors.

Influencing: The ability to communicate securely and flexibly makes it possible to influence both people and computer systems.

Sharing of information and data: The ability to store large amounts of data on powerful hardware combined with the ability to communicate securely and flexibly, makes it possible to share information and dataefficiently.

Photo: Shutterstock

POLITIET
KRIPOS

National Criminal Investigation
Service Postal address: PO Box 2094 Vika, 0125 Oslo
Street address: Nils Hansens vei 25, 0667 Oslo

Contact: +47 23 20 80 00 / kripos@politiet.no
Contact the police about cybercrime: https://tips.politiet.no/web/

Photo front page: Made with AI