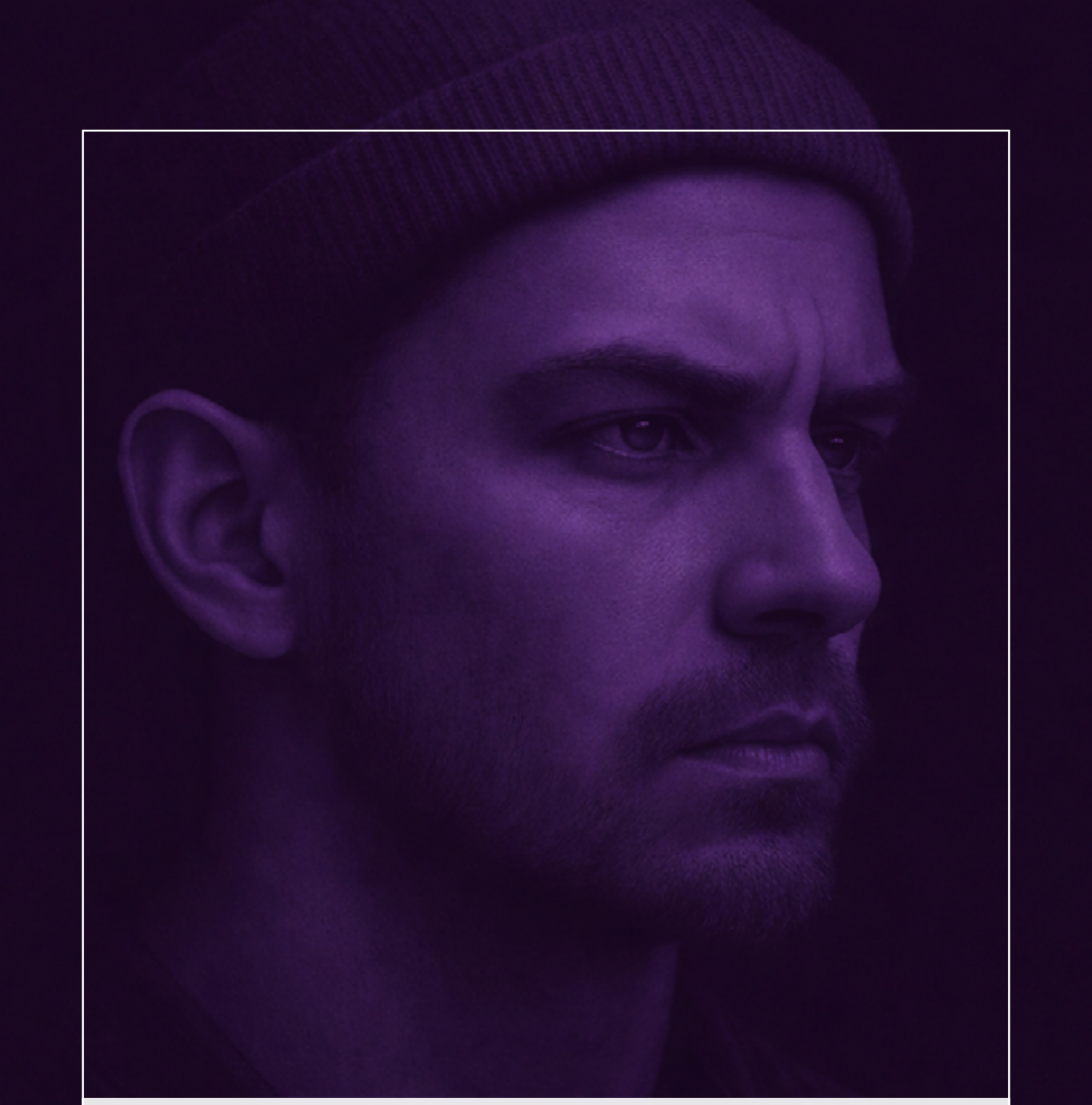
POLITIET
KRIPOS

Cybercrime 2026

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



Cybercrime 2026, NCIS
Annual police report on cyber-dependent and cyber-enabled crime

Layout: Økokrim
Print and number printed: 300x, Aksell
ISSN: 2704-2537

Photo: NCIS, AI-generated

Preface

The digital space has become an integral part of society. It influences how we communicate, work and organise ourselves, but also the ways in which crime is committed and how it evolves. *Cybercrime 2026* is the NCIS' contribution to shedding light on this landscape and to building a shared understanding of the threats, vulnerabilities and trends that affect society as a whole.

Ours is a time marked by geopolitical tension, technological transformation and an increasingly complex threat picture. War on the European continent, strategic rivalry between states and the increased use of hybrid means also affect the crime picture. Digital attacks, influence operations and exploitation of vulnerabilities in infrastructure critical to society often take place in the grey area between crime and security politics. Vulnerable children and adolescents are exploited in new ways and for a variety of reasons, with technology being both a driver and a means of exploitation. This places new demands on knowledge, cooperation and emergency preparedness.

The fact that 2026 has been designated the National Total Defence Year in Norway provides a unique context for this report. The term "total defence" refers to society's total ability to prevent, withstand and handle crisis and conflict. In this work, the NCIS and the police in general join forces with, and are mutually dependent on, public authorities, the business sector and civil society. Cybercrime challenges these dependencies by attacking the trust in and accessibility and integrity of digital systems.

This report shows that cybercrime can rarely be understood as isolated incidents. It is part of an ecosystem of actors, services and technologies in which commercialisation and division of labour is lowering the threshold for committing serious crime. It is, however, worth noting that crime in itself tends to follow established patterns, but with new means and an increased potential for harm. It is often in these shifts – rather than in the spectacular and entirely new – that the biggest challenges arise.

The main task of the NCIS is to prevent and combat organised and other serious crime. To achieve this in the digital space, we rely on knowledge, intelligence and cooperation, both at a national and an international level. Crime prevention is the underlying premise of this report, because early detection and targeted disruption of criminal structures are the most effective measures over time.

Cybercrime 2026 is intended as a source of information for decision-makers, subject-matter experts and partner organisations. It does not pretend to give all the answers, but aims to contribute to a shared situational understanding – a prerequisite for enhancing the overall resilience of our digitalised society at a time of unrest.

Kristin Kvigne
Director General of the National Criminal Investigation Service

Contents

Summary

Cybercrime 2026 provides a comprehensive and updated picture of the cybercrime situation in Norway, its characteristics, extent, and expected evolution, as seen from the police's perspective. The report springs out of the NCIS's responsibilities in the field of organised and other serious crime, and takes as its starting point a "normal state" including persistent trends and stable patterns of the threat landscape.

In this report, similar topics will be described in several chapters, but with differing perspectives and contexts. The main reason for this is that the NCIS endeavours to see cyber-dependent and cyber-enabled crime as part of a the larger crime picture, with common denominators and gliding transitions, rather than as separate, mutually exclusive phenomena.

One fundamental premise is that digital technology has become an integrated part and, often, a necessary requirement of modern-day crime. Consequently, the report does not draw a clear distinction between cybercrime and traditional crime, but describes a variety of crime along a continuum based on the degree of dependency on technology. The term "cybercrime" is here taken to mean crime where technology is either a target or a key enabler. This approach sheds light on how most serious forms of crime include digital components, and how the boundaries between the physical and digital domain are blurring.

The report discusses the *cybercriminal ecosystem* from the police's point of view and introduces a new analytical framework to help the understanding of the dynamics and approaches of various actors. Crime should not be understood as isolated actions, but as an interplay of actors, services, technology, market places and structural vulnerabilities. Commercialisation and division of labour has led to the emergence of a market where a variety of criminal services are offered for sale. This lowers the threshold for involvement and increases the scale and pace of crime. When we look at these phenomena as an ecosystem, it becomes easier to explain why measures targeting individual actors tend to have a limited effect if the underlying structures and enablers remain intact. The presentation of the cybercriminal ecosystem aims to highlight cooperation, dependencies and other links between actors, means and MOs. It will also discuss the nuances within specific groups of actors and point out the broad variety of, for instance, profit-driven cybercriminals.

In Norway, the normal state of cybercrime is still one dominated by profit-driven actors, sexual offenders and ideologically motivated

actors. Although digital fraud and cyber-enabled sexual crime constitute the bulk of the total case volume, cyber-dependent attacks against businesses and organisations also have a significant potential for harm.

The report emphasises that there are large uncertainties in the numbers, inter alia due to under-reporting and methodological limitations of some of the available data sources.

An important trend is the continued professionalisation of cybercrime. Criminal actors exploit scalability, automated solutions and access to new tools to streamline attacks and reduce risk. Artificial intelligence (AI) is highlighted as an important enabler, particularly when it comes to social engineering, automated tailoring of attacks and content production.

The report goes on to describe the emergence of new and more complex collaboration forms and coalitions among cybercriminals, particularly within the ransomware ecosystem. Such structures can help bolster capacity and potency but can also increase the actors' vulnerability through internal conflict and trust issues. An especially concerning trend is the emergence of extreme, violent online communities that constitute a considerable threat to children and adolescents through radicalisation, exploitation and pressure to commit self-harm and serious violence.

The police's role in the digital space is described as both crucial and challenging. Because cybercrime is characterised by anonymity, a fast pace and transnational activity, it places high demands on intelligence, analysis and international cooperation. The report emphasises prevention as the single most important measure, with a particular focus on early identification of trends, disruption of criminal structures and cooperation across sectors. Our legal access to coercive measures and our role in coordination with foreign authorities give the police a special role, but we are also reliant on contributions from other actors in society.

The last part of the report is an assessment of expected developments in 2026. The threat from cybercrime is deemed persistent and increasingly complex, both in terms of methods, actors and consequences. The long-term impact of small, gradual changes to the normal state can be considerable. Taken as a whole, the report provides a knowledge-based foundation for strategic assessments and underlines the need for a comprehensive understanding, continued adjustments and targeted prevention efforts faced with a dynamic and complex cyber threat picture.

Purpose of the report

For a number of years now, the NCIS has warned about the threat of online crime in all its forms. There is an increasing number of cyber-attacks, and the range of offences committed online is vast. The threat is unpredictable and global and affects all sectors of society. This makes coordination, information sharing and incident handling a challenge. In light of the current security situation, it is more important than ever to have a common knowledge basis and a shared strategic understanding of the national threat posed by cybercrime.

The NCIS has consequently decided to include the *normal state of cybercrime* in this year's report, in a bid to help the wider society understand and identify deviations, develop indicators and navigate in the continued efforts to prevent, avert, investigate and contain the damage occasioned by crime in the digital space.

Cybercrime can take on many forms, from basic crimes to advanced hybrid cyberattacks. The common denominator is the requirement for digital infrastructure and software.

As with previous issues, the purpose of this year's cybercrime report is to provide a better understanding of crime in the digital space, but also of what might be referred to as *cross-domain criminals*, who employ a combination of digital and analogue methods to optimise and streamline their activities and achieve their criminal goals.

Photo: Shutterstock

Our remit

The role and scope of the police

The police's mission, as laid down in the Police Act, covers both the digital and the physical space. Our mission comprises the prevention, detection, investigation and prosecution of cybercrime that may affect people, businesses, organisations and assets such as critical infrastructure in our country. Some key characteristics of cybercrime are that it tends to happen fast, virtually anonymously and across national and international jurisdictions. This means that to effectively combat cybercrime, close cooperation between public and private sector actors is required, both nationally and internationally.

The ambition and main strategy of the police is to prevent and deter crime, constantly staying one step ahead of the criminals. This calls for a systematic, structured and knowledge-based approach to prevention, and close inter-disciplinary partnerships across sectors.[1] In addition to the investigation of cybercrime – which, albeit its inherently reactive nature, can have a deterrent effect – and cooperation with law enforcement agencies in other countries, for example to identify new crime trends, the police have a number of different methods at their disposal in their efforts to prevent cybercrime. The methods span from presence on digital platforms to taking down digital infrastructure used to commit crimes. The efforts also include the development or adoption of technology and new techniques to help identify and deter crime. Intelligence production and knowledge sharing are important factors in the knowledge-based approach as they contribute to build a common understanding of the situation and build knowledge about the threat from cybercriminal actors.

Cybercrime as part of the NCIS's remit

The focus of the *Cybercrime 2026* report is closely connected to the remit of the NCIS, namely to "prevent and combat organised and

1 National Police Directorate (2021). *I forkant av kriminaliteten: Forebygging som politiets hovedstrategi (2021–2025).* p. 6. https://www.politiet.no/globalassets/dokumenter-strategier-og-horinger/pod/i-forkant-av-kriminaliteten.pdf

other serious crime"[2]. Furthermore, in order for crime to be considered cybercrime, its execution must be dependent on technology. Despite this, the divisions between some of these types of crime are not clear-cut, with some clearly qualifying as cybercrime whereas others do not, despite leaning heavily on technology to coordinate and streamline the criminal activity.[3]

As mentioned in last year's report, *crime targeting computer systems* and *crime committed in computer systems* did not exist before the advent of the digital space.
Crime committed in computer systems can be further divided into what the NCIS refers to as *cyber-dependent* and *cyber-enabled* crime. *Crime committed using computer systems and crime aided by computer systems* are conventional crimes occurring both in and outside of the digital space.

Crime targeting computer systems differs from other cybercrime in that it targets the computer system itself rather than the humans using the computer systems or the data held in the systems. Examples of this type of crime include computer intrusions and cyber vandalism. A computer intrusion is often a gateway to committing further crime in the computer systems.

Much in the same way as crime targeting computer systems, **crime committed in computer systems** only occurs in the digital space, but the latter targets the people using the computer systems or data held in the systems. Examples are creation of synthetic child sexual abuse material and cryptocurrency fraud. This is crime that, despite not targeting the computer systems themselves, cannot be committed outside the digital space.

Crime committed using computer systems is crime that is committed in the digital space, but which may equally well be committed in the physical space. Examples include romance scams, drug dealing, sexual extortion and hate speech in social media.

The last category is **crime aided by computer systems** – conventional crime committed in the physical world, but where computers are used as a supplementary tool. This is crime that is not usually included in the term "cybercrime" but which, in certain cases, overlaps with cy-

2 Prosecution Regulations. (1985). *Regler om ordningen av påtalemyndigheten* (FOR-1985-06-28-1679). Lovdata. https://lovdata.no/forskrift/1985-06-28-1679/§37-1

3 One example is violence-as-a-service (VaaS). Although technology is a prerequisite for this type of violent crime, it is not considered cybercrime.

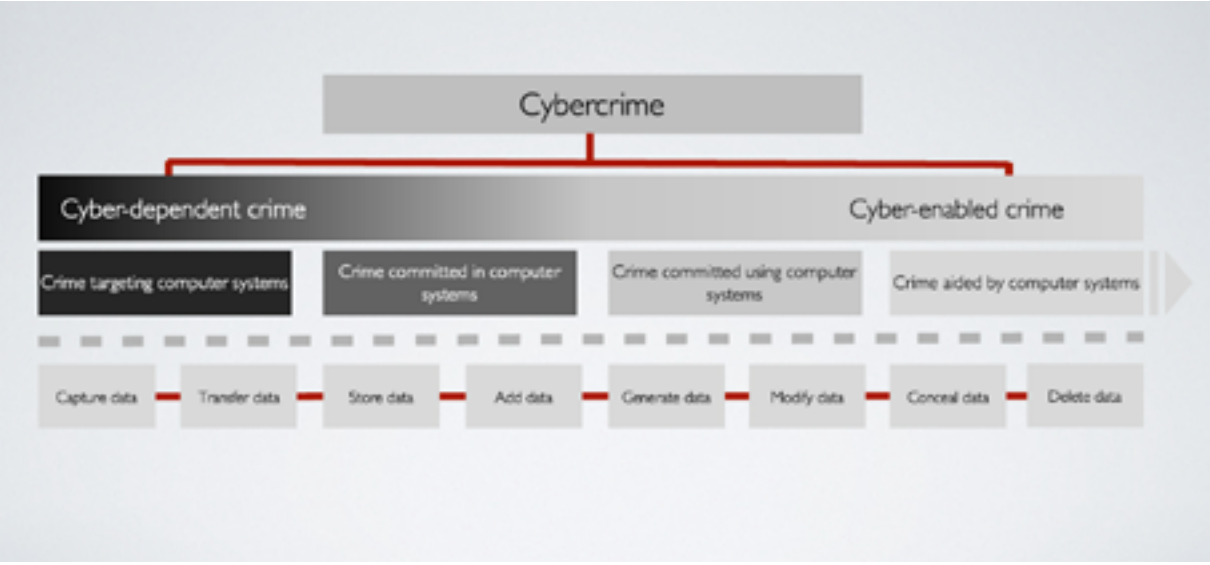


Figure 1: *The conceptual map* shows that cybercrime ranges from crime committed against computer systems to crime committed in the physical space but aided by computer systems. This is the full spectrum of cybercrime. The building blocks of cybercrime, as shown at the bottom of the diagram, are the basic activities that all kinds of cybercrime have in common, from one end of the spectrum to the other. Model prepared by the NCIS.

ber-enabled crime. Examples include criminals communicating via encrypted phones or messaging platforms, criminal networks recruiting young people into committing VaaS, and adults organising physical meetings with children on social media with the intention to commit sexual abuse. As a result of the widespread use of computer systems to commit crime, important evidence is now increasingly held by service providers and on digital platforms and devices. This produces a need for new skills and methods to fight all organised and serious crime.

Intelligence

The primary objective of intelligence is to support decision-makers and enable them to make well-informed decisions and implement measures. This is done by gathering, collating, analysing and assessing data which, in turn, are relayed to the party who commissioned the intelligence product. Intelligence production aims to improve the understanding of and insight into relevant threats. The purpose is to safeguard Norwegian interests and security and prevent, uncover and counter future threats.

Strategic intelligence aims to provide general insight into factors that impact national interests and security. The focus is on main developments such as trends, power dynamics, threats and opportunities set to shape the future. The objective is to enable the country and its people to act proactively.

A strategic alert is an advance warning of future threats and incidents with potentially serious consequences for national security and emergency preparedness, and is intended to help decision-makers implement measures before the situation escalates to an emergency. Strategic alerts are the results of long-term observations (gathering) and pattern recognition (analysis) and provide a basis for action.

Cyber intelligence differs from other areas of intelligence production in that it requires close integration with other disciplines, including other police disciplines, legal and technical experts. Although identifying vulnerabilities does *not* fall within the remit of intelligence work, vulnerabilities are sometimes uncovered through the analyses. It follows from this that cyber intelligence must take a comprehensive view of the threats (actors), vulnerabilities and assets and the relationship between them. Due to the inherent complexity, the development of models to help convey the internal relationships of the threats is a vital part of our work. This year, as in previous years, the NCIS has consequently developed new analytic frameworks and continued the work to develop a terminology of cybercrime as a contribution to the knowledge production within this field.

Photo: NCIS, AI-generated

Photo: Shutterstock

Cyberspace: distinguishing features and future relevance for organised and other serious crime

Technological innovation is the primary driver of change in the field of cybercrime. In this year's report, the NCIS therefore emphasises technology's bearing on the commission of various types of crime and describes the wider cybercriminal ecosystem[4] from this perspective.

The digital transformation takes place at different speeds across the levels and functions of society. Technological innovation is fast-paced, but fundamental human behaviour and institutional change tend to be much slower. This also applies to the police's own operations and our ability to implement new technology in our efforts against crime.

The digital space increases the scope and operational leeway for all types of crime. Whilst the digital space has increasingly become an integral part of crime, it also has some inherent characteristics that set it apart from the physical world. The digital space enables geographically and socially diverse actors to self-organise for optimal goal achievement throughout the value chain. A specific cyber threat may arise within a short space of time.

The digital space is man-made, under continuous construction and constantly changing. Moreover, it has proven to be fundamentally vulnerable and well-suited to criminal exploitation. This makes it particularly challenging to detect unwanted acts, identify perpetrators

4 See the conceptual map on page 11.

and uncover the actors' motives and intentions.

A strategically important characteristic of the digital space is the scaling opportunities, be it to compromise multiple computer systems simultaneously, generate vast amounts of content[5] or reach, exploit or manipulate large groups of people. Such actions, which would previously require significant resources and efforts, can now be automated in no time using digital tools.

Due to dependencies and *chains of trust*[6], be it in software and networks or between persons, organisations and functions of society, cyberspace also functions as a gateway to a vast array of assets.[7] As such, a single compromised network can constitute a strategically important threat or put lives in danger. In the previous issue of this report, the NCIS highlighted two strategic alerts: *chain attacks*[8] and *OT system attacks*[9] based on the potential for scaling and the potentially serious consequences for critical infrastructure and functions of society. A single attack by a single actor can consequently impact individuals, organisations and society as a whole.

We live in a society characterised by constant change, adaptation and new and emerging threats. The virtual world facilitates new, transactional collaboration between threat actors and new market places where criminal goods and services are traded. This enables criminals to implement rapid changes in terms of their organisation, type of crimes committed and approaches used.

---

5 E.g. text, audio, photo, video and source code.

6 A chain of trust is a sequence of dependencies in which trust is transferred from one step to the next, from a familiar and trusted source to something that could not otherwise have been verified directly. Source: SSL.com. (06.12.2021). *Hva er en sertifiseringsinstans (CA)?*. https://www.ssl.com/no/faqs/what-is-a-certificate-authority/

7 NCIS. (2025). *Cybercrime 2025*. pp. 35–42. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2025.pdf

8 Chain attacks provide criminals wanting to target a large number of victims with the opportunity to exploit vulnerabilities in shared or connected hardware or software.

9 Operational technology (OT) comprises systems, devices and communications infrastructure supporting the production, supply and maintenance of physical goods and services, often in industrial production facilities or other large process environments. OT also includes hardware and software used to control other systems or devices that monitor or alter physical processes.

Photo: Shutterstock

Cybercrime from a police perspective

Dark figures and other deficiencies in the police's data

The existing data on the different types of cybercrime are, in varying ways and to a varying degree, incomplete due to the amount of crime that goes unreported. This challenges the NCIS' capability to understand and describe the normal state. However, and despite these deficiencies, the NCIS has reasonable insight into parts of the cybercrime field, an insight we want to share to help build situational awareness in Norway.

The NCIS is aware that the number of unrecorded denial of service attacks[10] and computer intrusions not followed by other malicious activity or offences, is high.[11] Moreover, the *unreported crimes survey* from 2024 showed that only 24% of businesses and organisations that had been victims of computer intrusions and data theft had reported the offences to the police. The NCIS concludes from this that the number of unreported cases of cyber-dependent crime is high. Despite this dark figure, the NCIS has, in collaboration with the National Security Authority and private sector actors, gradually and over time compiled data to improve the

10 In a denial-of-service (DoS) attack, access to data, resources or services is blocked, wholly or in part, as a consequence of a targeted attack or unforeseen events. Source: Nätt, T. H. & Bartnes, M. (12.03.2025). *Tjenestenekt*. Store norske leksikon. https://snl.no/tjenestenekt

11 Cases where a computer intrusion has taken place but with no subsequent data theft or acts of vandalism (encryption), either because this was averted or because it has been established that the threat actor did not carry out any other malicious activities on the system.

statistical basis in the field of cybercrime.

Whilst various types of digital fraud[12] and sexual crime make up the bulk of recorded cybercrime, cyber-dependent crime constitutes a smaller proportion of the recorded crime. Certain types of cyber-enabled crime are less likely to be reported to the police.

Although cyber-enabled sexual crime includes certain offences that represent a high number of recorded criminal cases, this is an area of crime which, for a number of reasons, is also marked by under-reporting. One important reason is the delay in reporting sexual offences caused by psychological factors such as shame, guilt and fear. Many victims are also unaware that they have been the victim of a criminal act, or the matter is handled outside of the criminal justice system due to the young age of the offender. Moreover, there is a particular lack of knowledge about female offenders. In addition, there is a type of "dark figure" that is inherent to the police's own records: The chapter on sexual offences in the Norwegian Penal Code is technology neutral, meaning that it does not distinguish between offences that occur in the physical world and online. Practices also differ when it comes to the classification of criminal cases at receipt or filing of criminal complaints. It is therefore hard to obtain a full overview of the information already held by the police.

International trends in cybercrime

Globally, there has been an increase in all types of cybercrime. The one exception is hacktivism, for which numbers have remained consistently high for a number of years.[13,14,15] The main reason for this clear trend is the generalisation of

12 Digital fraud is a collective term for a number of malicious acts carried out on digital platforms with a view to manipulate, defraud or steal from individuals or organisations. It is the use of technology that separates digital fraud from other types of fraud.

13 The European Union Agency for Cybersecurity. (October 2025). *Enisa threat landscape 2025.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

14 Europol. (2025). *Internet Organised Crime Threat Assessment (IOCTA)*: Steal, deal and repeat – How cybercriminals trade and exploit you data. https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data

15 United Nations Interregional Crime and Justice Research Institute. (June 2024). *Beneath the surface: Terrorist and violent extremist use of the dark web and cybercrime-as-a-service* – June 2024. https://unicri.org/beneath-surface-terrorist-and-violent-extremist-use-dark-web-and-cybercrime-service-june-2024

AI tools and the increasing commercialisation of cybercrime. These two phenomena alone have increased the speed and efficiency of all types of cybercrime whilst, at the same time, making digital tools available to everyone present in the digital space.

All the same, it may be useful to look at some other *foreign* and *international* trends and developments to understand and alert to potential future developments within the field of cybercrime in Norway. Foreign trends and developments are changes that have yet to affect Norwegian individuals and organisations. International trends and developments are changes that take place in multiple locations around the world, including Norway, without regard to national borders. Such changes, relative to the situation described in the section about the normal state, form the basis for predicting what will happen in 2026.

Through the analysis and study of local and global circumstances[16] and developments, and the cooperation mechanisms[17] employed by criminals, the police will become better able to predict new threats, fight cybercrime and develop counter-measures with a profound and lasting impact.

Artificial intelligence (AI)

The advent of AI has led to the automation of a number of criminal tasks, such as the circumvention of security features, collation of large data volumes, scaling, forgery, translation and adaptation of text and speech, coding, pentesting and target selection. AI is used to make it harder to detect criminal activity, both through tweaking of software code and processes and through the introduction of a greater variety of attacks, making pattern recognition a less effective defence against crime. Additionally, social engineering based on audio and video content has recently taken a leap forward and become far more convincing. The improved quality adds a layer of credibility and makes it easier for actors to deceive and exploit other people, including children. AI drives new crime trends, helps inexperienced criminals with limited skills and contributes to the overall growth in crime.

16 For example state control over the population's use of the Internet, poverty, internet access, computer literacy, history, culture etc.

17 Mechanisms affecting how criminals cooperate.

Photo: Shutterstock

In previous issues of *Cybercrime*, the NCIS discussed the emergence of AI agents[18] and predicted that the surge in volume of cyber-dependent crime would only occur once AI systems[19] became able to autonomously commit crimes and criminal activity on behalf of humans. Recent developments in agentic systems[20] have taken the technology one step closer to this turning point, and it is already possible to fully automate technological tasks that used to require human involvement. This is directly transferable to crimes committed using computer systems.

Partial assessments

It is *likely* that demand for criminals with AI skills will increase in parallel with the increased scope to use AI to commit cyber-dependent crime. Whilst AI and crime-as-a-service (CaaS)[21] reduce the need for technical skills and set the bar low for cyberattacks, it is *likely* that the use of AI models by criminals will lead to mistakes and disclosures which may help the police identify the criminal actors. It is *likely* that criminals with basic technical skills are at the highest risk of being exposed based on their use of AI.

---

18 AI agents can be described as automated robots that, independently or in collaboration with other AI agents or humans, can carry out technological tasks autonomously or guided by humans. This includes the use of digital tools and control of computer systems.

19 AI systems is a collective term for different kinds of software and hardware that carry out actions, physically or digitally, based on the interpretation and processing of structured and unstructured data for the purpose of achieving a given objective. Source: Ministry of Local Government and Modernisation. (2020). *Nasjonal strategi for kunstig intelligens*. p. 9. Government of Norway. https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/no/pdfs/ki-strategi.pdf

20 Other AI systems may also have agentic capabilities without necessarily being referred to as AI agents. Such capabilities include objectives, actions, memory and rethink.

21 Crime-as-a-service (CaaS) is the buying and selling of criminal services, software and tools. CaaS contributes to making crime profitable, financing new crime and making crime more accessible, including to actors who are unable to commit such crimes on their own.

Photo: NCIS, AI-generated

Increased commercialisation of cybercrime

Increased commercialisation means that cybercrime is becoming more professionalised, widespread and common, in Norway as in the rest of the world.[22] The offer of cybercriminal products and services is growing, particularly in the form of ready-made product packages[23], rental and subscription services, consulting and customer support. A vast grey area is emerging in the commercial part of the cybercriminal ecosystem, where professional actors sell expertise and tools without themselves taking part in the criminal activities. The cybercriminal ecosystem is to a greater or lesser extent dependent on such facilitators – persons who, drawing on their expertise and access, contribute to committing or concealing crime.[24]

During autumn 2025, the concept of violence-as-a-service (VaaS) was brought to the attention of the wider public in Norwegian. The NCIS notes that experience from abroad shows that VaaS has some prominent digital elements. Recruitment, planning, coordination and payment all tend to take place in the digital space. Additionally, doxxing[25], harassment, surveillance and sabotage may all escalate into physical harm. The trend has much in common with the commercialisation of ransomware and phishing attacks previously observed in Norway, and the same digital platforms are used.

Emergence of new coalitions and partnerships

2025 saw the establishment by existing international cybercriminal networks of new coalitions of so-called ransomware-as-a-service

22 Europol. (2025). *Internet Organised Crime Threat Assessment (IOCTA)*.

23 Product packages can e.g. include access to infection and anonymisation tools and a secure payment channel.

24 National Criminal Investigation Service. (2025). *Cybercrime 2025*. p 11.

25 *Doxxing/doxing* is the publishing of personal details or sensitive data about a person or organisation.

operations (RaaS operations).[26, 27] A number of the ransomware applications that are now part of these new coalitions were used to attack Norwegian businesses and organisations in 2025.

Cybercriminal threat actors announcing new partnerships is nothing new, but this kind of cooperations have previously brought about changes in MO.
When such new partnerships cause a significant shift in capacity, one should take notice.

One of the coalitions formed in 2025 and now going by the name of *Scattered Lapsus$ Hunters*, has reportedly adopted a greater variety of techniques to gain access to organisations' systems. We do not know the full extent of this, but according to reports, the group now targets employees of businesses and organisations with vishing, or voice phishing[28], to obtain access to systems and data. The NCIS are not aware of any examples of vishing in connection with computer intrusions into organisations in Norway. The use of this technique would represent a deviation from the normal state in Norway.

Criminals from the Scattered Lapsus$ Hunters have in statements to media claimed responsibility for a number of cyberattacks against well-known international corporations.

---

26 Ransomware-as-a-service (RaaS) is a sub-category of CaaS involving sale or rental of an existing ransomware.

27 Examples are Scattered Spider, LAPSUS$ and ShinyHunters, which have merged to form the "Scattered Lapsus$ Hunters". DragonForce has also announced on its leak pages that it has merged with Qilin and LockBit to form a new coalition. Sources: Culafi, A. (08.10.2025). *LockBit, Qilin & DragonForce Join Forces in Ransomware Cartel*. Dark Reading. https://www.darkreading.com/cyberattacks-data-breaches/extortion-gangs-join-forces-ransomware-cartel and Picus Labs. (20.10.2025). *Scattered LAPSUS$ Hunters:* 2025's Most Dangerous Cybercrime Supergroup. Picus Security. https://www.picussecurity.com/resource/blog/scattered-lapsus-hunters-2025s-most-dangerous-cybercrime-supergroup

28 Vishing, or voice phishing, is a type of phishing where cybercriminals use phone calls (and potentially voice technology) to manipulate their victims into disclosing sensitive information.

Partial assessments

Established cybercriminal networks may wish to establish new partnerships for a number of reasons. It is, however, *likely* that increased capacity through the pooling of resources, infrastructure, competencies and experience contributes to a considerable shift in capacity, and there is *an even chance* that this is a desired outcome on the part of the network.

It is further *likely* that the mergers of well-established names in the ransomware-as-a-service ecosystem and their subsequent statements about this to media outlets, is a matter of branding based on the idea that high-profile cybercriminal networks are more likely to be perceived as a potent threat. There is *an even chance* that this can increase the victims' willingness to pay a ransom.

There is *an even chance* that newly-established coalitions, such as the Scattered Lapsus$ Hunters, will focus on attacking large organisations of great symbolic value as part of their branding efforts. There is *an even chance* that this development will also impact Norwegian organisations in the form of more targeted cyberattacks.

At the same time, it is *likely* that more partnerships and temporary alliances amongst RaaS groups will create new lines of conflict and increase rivalry between criminal actors. There is *an even chance* that this will lead to more cases of doxxing – internal leaks and criminals publishing details about their peers.

If the reports of vishing used in connection with computer intrusions are correct, it is *likely* that the technique will also be used against private and public sector organisations in Norway from 2026 onward. It is *highly likely* that vishing is perceived as more credible than other phishing techniques, and it is *likely* that this will contribute to a higher success rate for cybercriminals seeking to obtain user credentials or sensitive information. There is *an even chance* that synthetic, AI-generated voices will have the same effect as genuine human voices, depending on the level of realism.

The Com: extreme, violent online communities

In February 2025, Europol published a report[29] warning about a recorded global increase in the scope and extent of the extreme, violent online communities sometimes referred to as "cults". The trend was confirmed by the National Center for Missing and Exploited Children (NCMEC), who stated that they in 2022 had received fewer than 100 tip-offs about the phenomenon, but that the number had risen to 200 in 2023, 1300 in 2024 and more than 1000 tip-offs in the first half of 2025. The phenomenon introduces a new sub-group of uncategorised actors with varying motivations, who present a threat to children online. Read more about the prevalence of this phenomenon on pages 46–48.

Global geopolitical tensions

The victims may be local, but cybercrime is, by its very nature, a global phenomenon. It is therefore crucial to take a wider perspective and look beyond national borders to get an idea of the potential threats facing Norwegian individuals, organisations and society as a whole. This section is dedicated to geopolitical tensions that have not yet been observed in Norway, but that are likely to impact cybercrime in Norway, either directly or indirectly.

Extreme, violent online communities or "cults" have emerged as a global phenomenon. The various online communities are offshoots of *The Com*, short for *The Community*, which is the main network internationally. The actors' motivation is unclear, but overlapping interests including nihilism, occultism, extremism and child sexual abuse have been described. Some of these online communities have links to the extreme right-wing circles that praise the use of terrorism and violence as a means to "destroy society". The communities spread extreme, violent content, exploit vulnerable children and adolescents and groom them into performing extremely serious acts on themselves and others. On an international level, several of these groups have been categorised as terrorist organisations.

29 Europol. (2025). *The rise of online cult communities dedicated to extremely violent child abuse.* https://www.europol.europa.eu/cms/sites/default/files/documents/IN_The_rise_of_online_cult_communities_dedicated_to_extremely_violent_child_abuse.pdf

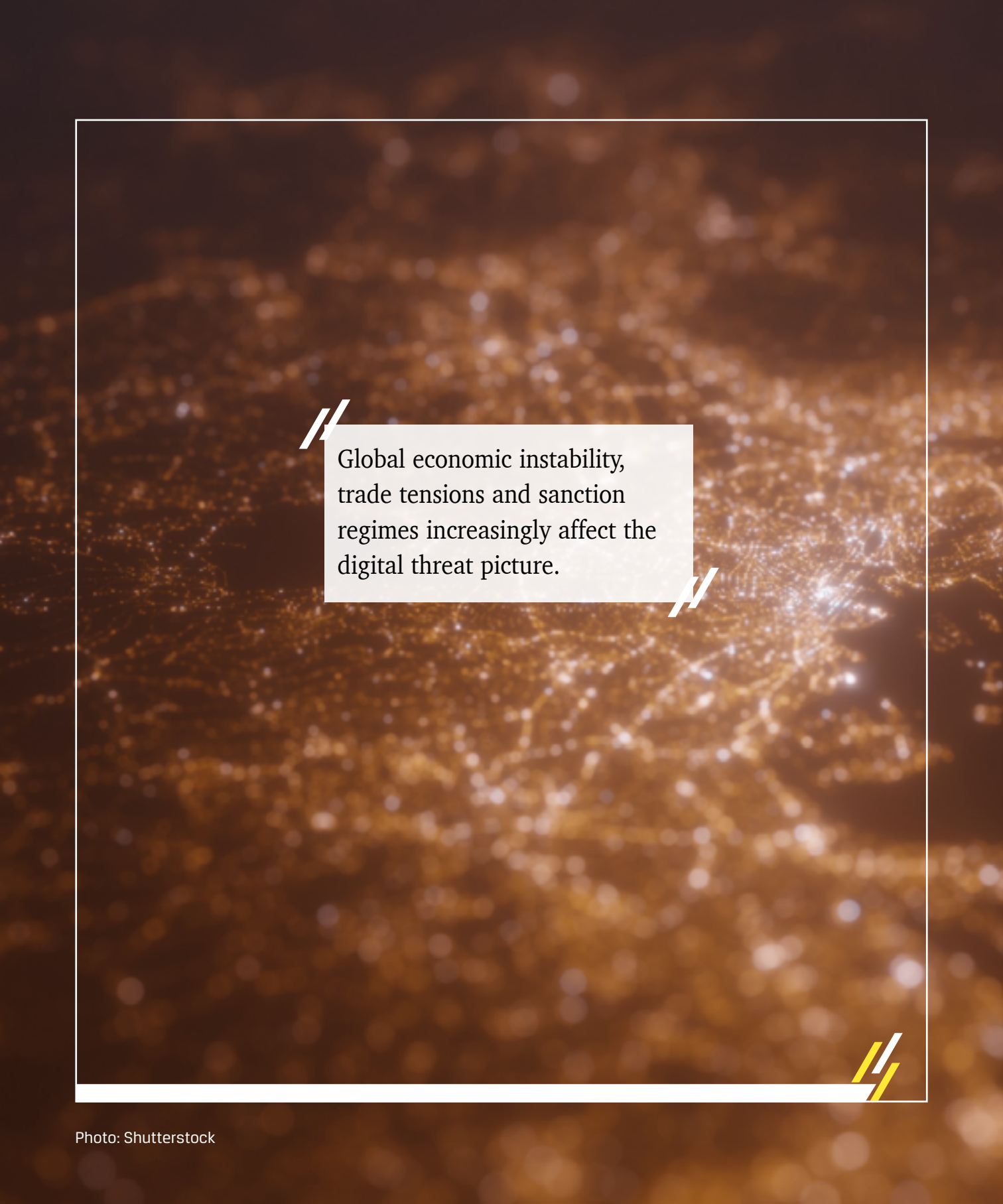


Photo: Shutterstock

Physical wars and regional armed conflicts have in recent years highlighted the position of cyberspace as an integral part of modern warfare. Technological advances happen fast, not least in Russia's war against Ukraine. Experience and tools from such conflicts can quickly be distributed and implemented by actors with entirely different motives. In this way, events in one part of the world can have a bearing on available knowledge, capacities and threat activities far beyond the geographical boundaries of physical conflicts.

Global economic instability, trade wars and related political tensions and sanction regimes increasingly affect the digital threat level. Trade wars, for example between the USA and China, contribute to driving up costs, creating supply shortages and altering the market for digital services and security solutions. This can make it harder for organisations to maintain the required level of cybersecurity, whilst creating new opportunities for criminals who offer cheaper, but unsafe, alternatives.

In parallel to this, there is an ongoing global race in which major world powers, in particular, compete for domination in fields such as advanced infrastructure, quantum computing and artificial intelligence. Competition stimulates innovation but also contributes to increased fragmentation of digital systems and more complexity. This creates an increasing number of gateways susceptible to be exploited for criminal purposes by state[30] and private sector actors. Another consequence of the innovation is increased experimentation with methods and tools, which can be quickly spread across actor types and national borders.

Overall geopolitical tensions contribute to a more unpredictable cyber threat picture. Factors in other countries impact both the volume, character and complexity of cybercrime. As the crime cannot be contained by national borders, the consequences of international conflicts, economic fluctuations and technological rivalry are also noticeable in Norway.

Partial assessments

There is *an even chance* that the technology that is currently being developed for hybrid warfare will be used to commit criminal offences against Norwegian targets in 2026.

There is *an even chance* that economic pressure and sanctions may also increase the incentives to commit profit-motivated cybercrime amongst individuals, groups and state actors alike.

30 The term "state actor" is used to designate a national state that constitutes a threat or that commits cybercrime.

Financially motivated sexual extortion

In other countries, there have been indications that perpetrators behind financially motivated sexual extortion, also known as "sextortion", share or sell the material as sexual abuse material, probably to increase profits. Although this phenomenon is hitherto unrecorded in Norway, it was outlined as a potential future trend in the *Cybercrime 2023*[31] report.

Selection of targets

Target selection by cybercriminals is changing rapidly and several clear trends are emerging.

The range of organisations targeted by cyberattacks is expanding rapidly. One clear trend is to first obtain personal details that are subsequently used to gain "legitimate" access to the systems. This means that the attacker exploits a number of physical and digital attack vectors to get to their target, such as email, social media, websites, phone calls, physical access cards and in-person attendance.[32, 33, 34] This means that the attacker exploits a number of physical and digital attack vectors to get to their target, such as email, social media, websites, phone calls, physical access cards and in-person attendance. Criminals exploit the fact that their targets navigate between a number of different channels to increase their chances of succeeding with the attack. The NCIS also notes that cybercriminals seem to be drawn to countries with weak law enforcement and tend to use these countries as a base for their activity.[35,36]

---

31 NCIS. (2023). *Cybercrime 2023*. p 19. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

32 Sometimes referred to as *omnichannel attacks* or *multi-channel attacks*.

33 Telenor. (October 2025). *Digital sikkerhet 2025: Vi må ruste oss*. p. 28. https://www.telenor.no/binaries/om/digital-sikkerhet/2025/sikkerhetsrapport_tjuefem.pdf

34 Sopra Steria. (2025). *State of cyber security 2025,* pp. 11, 13, 19. https://www.soprasteria.no/docs/librariesprovider2/sopra-steria-no-documents/rapporter/sopra-steria-state-of-cyber-security-2025.pdf

35 Interpol. (23.06.2025). *New INTERPOL report warns of sharp rise in cybercrime in Africa*. https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa

36 Ecofin Agency. (30.09.2025). *Cybercrime Costs Africa $3B as Interpol Flags Legal, Cooperation Gaps*. https://www.ecofinagency.com/news/3009-49122-cybercrime-costs-africa-3b-as-interpol-flags-legal-cooperation-gaps

One clear trend is to first obtain personal details that are subsequently used to gain “legitimate” access to the systems.

Photo: Shutterstock

Recently, more cybercriminals have turned their attention to organisations with integrated OT–IT systems.[37] Such systems may be deliberately or inadvertently attacked, in some cases by actors with no particular technical skills. But as discussed in *Cybercrime 2025*[38], for a destructive attack[39] on an OT–IT system to be successful, advanced techniques must be applied. The potential profits yielded by a successful attack means that it may be worth putting in a considerable extra effort. One example of a recent successful attack was the attack against Jaguar Land Rover that led to a five-week shutdown and a financial loss currently estimated at in excess of 25 billion Norwegian kroner.[40]

This seems to coincide with another international trend whereby more advanced criminals move away from quantitative attacks towards a more targeted process using data, often from previous data thefts, to identify their prime victims[41].

The attack against Collings Aerospace, which among other things resulted in the shut-down of automated check-in and bag reclaim systems and long delays at airports in London, Berlin and Brussels, is a good example of how a third-party supplier[42] can become a gateway to critical infrastructure. Increased efforts by cybercriminals to target OT–IT systems may be part of the bigger picture.

This last trend indicates that the bulk of cybercrime is committed by new, inexperienced and less competent actors supported by AI and commercially available software, whereas more sophisticated cybercrime is committed by a relatively small number of experienced, extremely competent individuals.

37 The European Union Agency for Cybersecurity. (October 2025). *Enisa threat landscape 2025*, p. 9.
38 NCIS. (2025). *Cybercrime 2025*. pp. 55–59.
39 See the definition of destructive attacks on pp. 43–44.
40 Jaguar Land Rover. (19.09.2025). *Letter from Jaguar Land Rover relating to the cyber attack on the company*. https://api.parliament.uk/committees/publications/49616
41 Prime targets are generally key personnel, third-party suppliers with access and decision-makers in the supply chain.
42 A third-party supplier is a business or organisation that supplies logistics services such as imports, storage and delivery of goods and services on behalf of others.

Photo: NCIS, AI-generated

> The cybercriminal threat consists of a plethora of digital attack forms and criminals taking advantage of technological vulnerabilities, exploiting system access and manipulating people.

Photo: Shutterstock

Partial assessments
There is *an even chance* that businesses targeted by cyberattacks in 2026 will be subjected to simultaneous attacks in multiple channels. When an organisation becomes a victim of a multi-channel cyberattack, it is *likely* that several cybercriminals or cybercriminal groups are behind the attack due to the tendency towards increased specialisation amongst cybercriminals.

There is a tendency amongst cybercriminals to prefer public sector targets. This is *likely* due to the combination of legacy systems[43], limited resources and inferior technological competence in the public sector, paired with the management of complex technological solutions, making these organisations vulnerable to digital attacks.

The normal state of cybercrime in Norway

This section outlines the *normal state of cybercrime* as seen from the NCIS' and the police's perspective. The term "normal state" is here taken to mean the current cybercrime situation, including lasting trends that have been present for several years. The normal state of cybercrime in Norway is not an exact mirror image of reality but, rather, a rendering of some typical features of various crime types that form part of this reality.

The normal state functions as a benchmark, enabling us to identify deviations and trace the evolution of crime. This limits the risk of unpleasant surprises and prepares us for and enables us to better handle future challenges.

The cybercrime threat consists of a plethora of digital attack forms and criminals who exploit technological vulnerabilities and system access and manipulate people. Cybercrime in Norway is still dominated by profit-motivated criminals, sexual offenders and hacktivists[44]. The criminals are adaptable, and the threat they present is dynamic and constantly evolving at the pace of digitalisation of society and the

43 "Legacy systems are old, often outdated systems that are vulnerable to exploitation because they were developed at a time when the security situation was very different."

44 A hacktivist is an actor (individual or group) who commits criminal acts in the digital space to convey a religious, political or other ideological message. The term is not to be confused with the domain-neutral "activist", which does not necessarily imply anything criminal.

emergence of new technologies. It encompasses both simple and complex modi operandi and ranges from automated mass attacks to targeted, sophisticated operations.

Hacktivism is politically or ideologically motivated illegal digital activism that aims to affect social change, challenge established power structures, influence opinion, weaken the credibility of opponents or further a specific cause or identity.

The normal state of cyber-enabled sexual crime in Norway

Although sexual crime has always existed and constitutes a persistent threat to children and young people, technological developments have significantly changed their nature. Offenders increasingly take to digital platforms to groom their victims and commit and document the abuse, and the technology provides new possibilities for anonymisation and evasion of prosecution. The internet has not only enabled online commission and broadcasting of traditional child sexual abuse, it has also brought about new types of sexual crime that are entirely dependent on the internet. This contributes to a more complex and nuanced normal state and places greater demands on police and other actors of society in terms of prevention, detection and prosecution of sexual crime.

Child sexual abuse is a high priority for the NCIS. Many cyber-enabled sexual crimes are directed at children, who are approached online by sexual predators who go on to abuse them sexually. In the vast majority of cases, perpetrators approach and sexually exploit their victims on generally available social media, but children can also be befriended on chatroulette or gaming platforms Each year a number of children are also exploited sexually on end-to-end encrypted communication platforms. Finally, the normal state includes Norwegian actors who purchase self-generated sexual content from Norwegian children. Last year the NCIS reported an escalation of this phenomenon, warning that many of the actors had a history of sexual offences against children, some of them with a very serious criminal record of violence and sexual crime.[45]

The sexual offences committed online range from sexually offensive conduct to rape. Many of the cases culminate in sexual chatting, indecent exposure online and the offender making the child send them nude photos and videos, sometimes against payment. In many cases it is uncertain how far the offender would have been willing to go if the contact had not been

45 NCIS. (2025). *Cybercrime 2025*. p 84.

> Offenders increasingly take to digital platforms to groom their victims and commit and document the abuse, and the technology provides new possibilities for anonymisation and evasion of prosecution.

Photo: Shutterstock

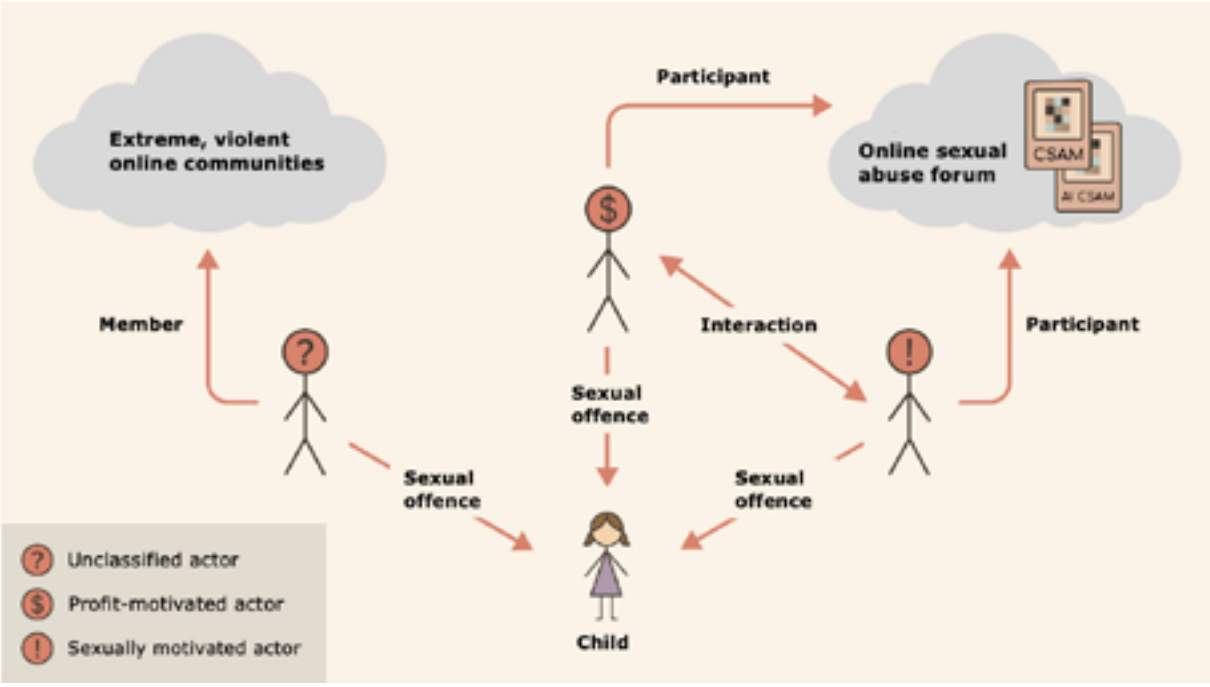


Figure 2: *The ecosystem of cyber-enabled sexual crime*. Bottom centre is a child, surrounded by sexually motivated, financially motivated and uncategorised actors (cult members) who subject the child to various types of sexual offences and interact with other actors, whether these share their motivations or not. CSAM stands for Child Sexual Abuse Material, and AI CSAM is synthetic, AI-generated child sexual abuse material. The model is developed by the NCIS.

broken off. When a child engages in sexual acts with themselves in a photo, video or live video chat, the offence canqualify either as a sexual act, sexual activity or rape.

Some cases culminate in the victim being subjected to sextortion. The extortion can result in a number of different offences, committed for a variety of motives. A common approach is that the offender tricks the child into sharing a nude photo of themselves and then uses the photo as a means of pressuring the child in order to achieve a desired outcome, such as receiving more photos and videos of a sexual nature. The use of synthetically generated images has also been recorded in such contexts. Until recently, sextortion was a type of crime targeting financially able adult men. In the last five years, however, some of the

victims have been boys under 18, and this has now been included in what the NCIS considers to be the normal state.

Norwegian perpetrators produce, store, share, buy and sell child sexual abuse material (CSAM). The production consists of the documentation through photos and videos of contact and non-contact (online) sexual abuse. Sharing and trading happens both on the open internet and on the darknet, on file sharing networks, file exchange services, social media and end-to-end encrypted communication platforms. CSAM is most often swapped and shared at no charge, but users who pay for such content tend to use cryptocurrency or a range of different payment services including payment providers.[46] Norwegian actors also produce, obtain and share synthetically generated CSAM.

Live distant child abuse (LDCA) is committed by a few hundred to a thousand Norwegian perpetrators each year. The victims are mainly children, primarily girls, in high-risk countries, most often the Philippines. Contact is often established through pornography websites offering live-streaming of adult sexual content, where the perpetrators are offered to buy live distant child abuse. Many LDCA buyers actively seek out the websites with a view to purchasing LDCA, but there are also what appears to be opportunistic cases, with perpetrators accepting to buy LDCA when they are offered it, and sellers being very persistent when approaching potential customers. LDCA often happens on ordinary, commercial platforms offering video chat and file exchange solutions. LDCA is typically purchased through commonly available payment solutions and is not considered an advanced type of crime. Some actors do, however, pay for LDCA with cryptocurrency.

Although sexual crime amplified by or committed in the digital space targets Norwegians of all ages, children between the ages of 13 and 15[47] are especially vulnerable to sexual exploitation. Girls are over-represented in the statistics, but there are also boys amongst the victims. For example, more boys than girls become victims of sextortion.

The vulnerabilities enabling the sexual abuse are as numerous as they are complex. Due to their young age, the victims – children – lack consequential thinking and awareness of the potential risks and dangers, especially online. Digital platforms function as a door from the child's bedroom to the rest of the world. It is

46 Payment providers are services used to transfer payment between two parties, taking on the role as an intermediary. Examples of such services are Vipps (Norway) and PayPal.

47 The average age of children who fall victim to cyber-enabled child sexual abuse is 14, whereas the average age of child victims of sexual abuse overall, is 12.

easier to deceive a child online and, for example, hide behind a fake identity or pose as someone of a different age and gender. Parents and other trusted adults do not always have the knowledge required to protect the child and prevent child sexual abuse, a fact which is actively exploited by offenders. Platforms that attract children with features such as games, music and interaction with friends, facilitate contact with strangers, and sexual offenders seek out arenas where they are sure to find children, whether online or in the physical world.

Cyber-enabled sexual crimes cause great harm to individuals. Each child victim is not only the victim of a crime, but potentially also has to live with far-reaching, lasting consequences. Together, all the individual destinies add up to a major societal problem. Moreover, the macro-economic costs of these crimes are high as they impact not only the children's schooling and education, but also their future careers and health and their ability to establish and maintain interpersonal relationships.

The normal state of cyber-dependent crime in Norway

Cyber-dependent crime is a persistent threat to individuals and private and public sector organisations in Norway. Various combinations of computer intrusions, data theft, extortion and computer vandalism are still the main approaches used by profit-motivated criminals involved in cyber-dependent crime. In cases where individuals fall victim to a computer intrusion, it is the victims' private email accounts, social media user names and cloud storage solutions that are targeted.

The normal state also includes the use of various kinds of ransomware in attacks against Norwegian organisations. The type of ransomware employed varies and changes over time as new variants emerge and others disappear or re-emerge under a new name.[48] The approach used by criminals committing ransomware attacks has remained relatively stable over several years and includes computer theft, encryption of the organisations' systems, or a combination of both. This is then used as a basis for further extortion.

Data theft is common following intrusion into the computer systems' of private individuals or organisations. The NCIS has seen examples of information stolen from organisations being made available online on various forums and platforms. However, this is not a regular occurrence. Although threat actors often threaten to publish data, they more often than not do not go through with it. Whether and how the data stolen from organisations and individuals are

48 Such ransomware is often used by criminals who obtain it through a RaaS business model.

used to commit further crime, is uncertain, but this does nonetheless constitute a persistent threat to individuals and organisations.

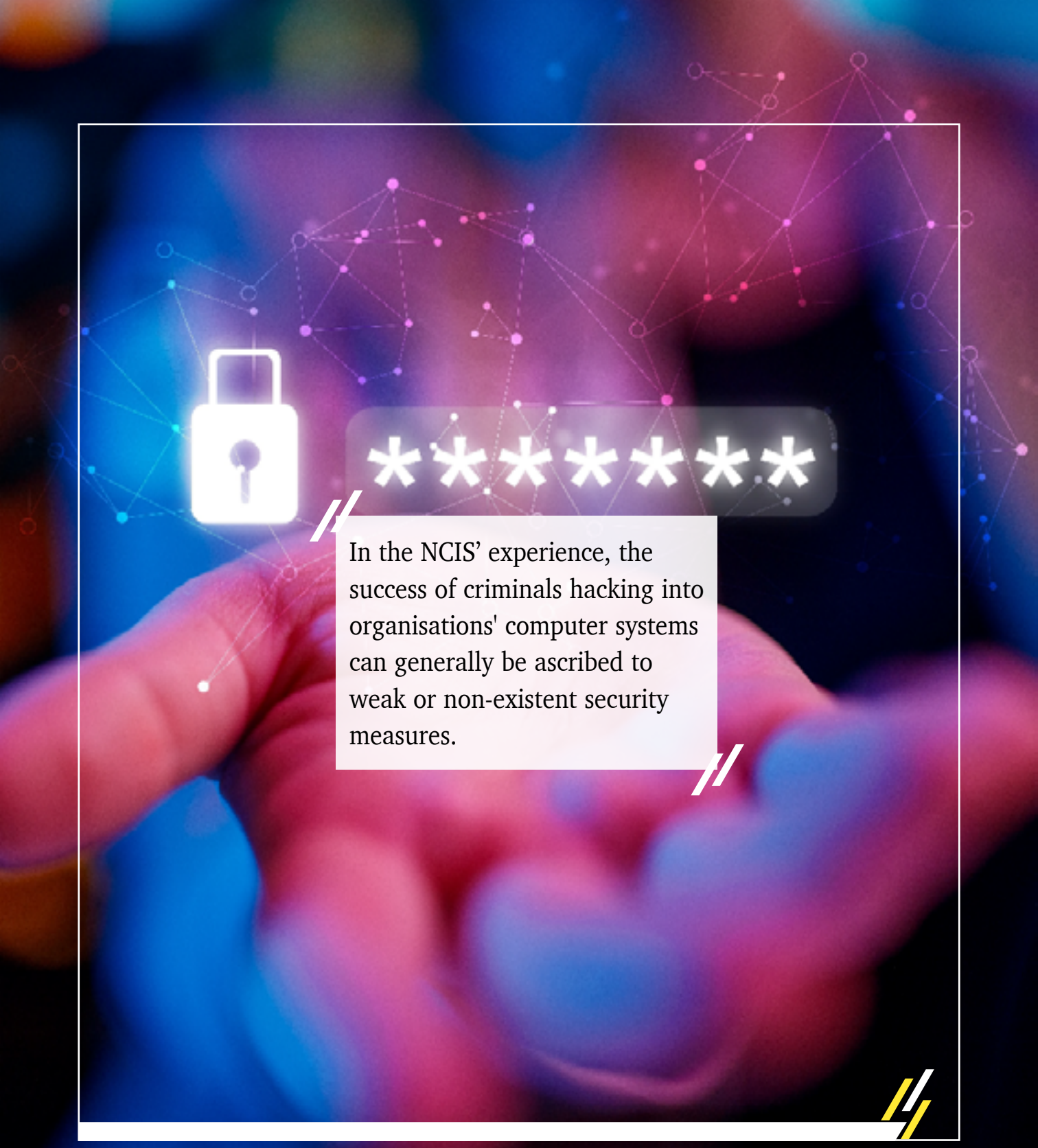
Denial-of-service attack (DoS) is still the most widely used form of attack used by hacktivists. The attacks are often ideologically motivated and aim to create unrest, influence public opinion and weaken trust in Norwegian institutions. This attack type is widespread, frequent and can be committed by actors with only limited technological skills. Beyond temporary service outages and minor disruptions, DoS attacks rarely have serious consequences for victim organisations. However, repeated campaigns can put operations under great strain, increase emergency preparedness costs and damage the organisation's reputation.

Digital fraud comes in many different forms and, depending on how it is done, can have elements of both cyber-dependent and cyber-enabled crime. It can be directed at organisations as well as individuals, and the victims are an extremely diverse group. Digital fraud still accounts for a large volume of crime, and the financial losses generated by this this type of crime are substantial.[49]

In the NCIS' experience, the success of criminals hacking into organisations' computer systems can generally be ascribed to weak or non-existent security measures. To gain initial access, criminals most often either login[50] to the organisations' systems or exploit existing vulnerabilities. The NCIS has seen fewer examples of threat actors gaining access through

49 In 2024 the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim) estimated the criminal proceeds of digital fraud at more than NOK 2 bn (around EUR 180 m). Source: Ministry of Justice and Public Security. (18.11.2024). *Økt innsats i kampen mot svindel på nett*. Government of Norway. https://www.regjeringen.no/no/aktuelt/okt-innsats-i-kampen-mot-svindel-pa-nett/id3117017/

50 The most commonly observed login techniques are the use of legitimate user credentials that have been stolen or otherwise taken from someone with system access, either through social engineering or through the use of infostealer malware. Brute-force attacks are another known method used to guess the login details of users who either have weak passwords or lack multi-factor authentication.



> In the NCIS' experience, the success of criminals hacking into organisations' computer systems can generally be ascribed to weak or non-existent security measures.

Photo: Shutterstock

back doors[51] or insiders[52], although this also happens occasionally.

Weak or non-existent security measures may include weak passwords, lack of multi-factor authentication, infrequent system updates or a vulnerable infrastructure that is exposed to the internet. In the absence of a security culture, the organisation may fail to detect or patch such vulnerabilities, which again exposes the organisation to cyberattacks.

The potential for harm caused by cyber-dependent crime varies depending on the type of attack, the target and the affected assets[53]. From the authorities' point of view, cyber-dependent crime directed at critical infrastructure and vital services and utilities is a serious and persistent threat. Downtime and outages of vital services and manipulation of OT systems can impact the physical world and put life and limb in danger. Cyberattacks committed with the sole purpose to destroy or sabotage business operations are often referred to as *destructive cyberattacks*. This type of attack is typically committed using malware known as *wiper malware*, which permanently deletes or destroys data, and consequently has a great

51 The term "back door" is used to refer to a way into a system which has been opened by an unauthorised party or left open by mistake, unbeknown to the system owner. Through such a back door, actors may be able to read, amend or delete information. Source: Nätt, T. H. (15.01.2024). *Bakdør*. Store norske leksikon. https://snl.no/bakd%C3%B8r

52 The term "insider" is here taken to mean a current or previous employee, consultant or contractor who has or has had legitimate access to the organisations' systems, procedures, objects and data, and who misuses their knowledge and access to carry out actions that harm or cause a loss to the organisation. Source: Norwegian National Security Authority. (2023). *Temarapport: Innsiderisiko*. p. 9. https://nsm.no/getfile.php/133153-1591706148/NSM/Filer/Dokumenter/Rapporter/Temarapport%20innsidere.pdf

53 An organisation's assets can be material or immaterial, e.g. physical objects that the organisation relies on to fulfil its purpose, or data it possesses. Source: Norwegian National Security Authority. (2020). *Grunnprinsipper for sikkerhetsstyring*. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/identifisere-og-kartlegge/identifisere-verdiene/

potential for harm. It is, however, unusual to see this kind of malware used in other contexts than war and conflict, and the NCIS is not aware of any examples of Norwegian organisations targeted by destructive cyberattacks. Although cyberattacks involving ransomware can have extremely serious consequences for the victim organisations, this is not the same as destructive cyberattacks. Whereas destructive cyberattacks are usually used to commit sabotage, encryption is used to obtain a means to extort the victim in a profit-motivated attack.

Cyber-dependent crime directed at individuals can have serious consequences for individual victims. Personal and sensitive information[54] coming into the wrong hands is one of the most common consequences of cyber-dependent crime targeting individuals.

The Covid pandemic brought about a closer integration between the personal and professional sphere as many moved their place of work to outside the organisation's traditional physical set-up and protective measures. As a result, the vulnerability surface has expanded, and so has the scope of criminal actors to exploit private individuals to access enterprise systems.[55] As a consequence of this integration between the personal and the professional, a threat to individuals must also be seen as a threat to organisations.

54 An individual's personal and sensitive information can, e.g., include health information, personal photos and documents.

55 NCIS. (2024). *Cybercrime 2024*. p 52. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf

Partial assessments

The NCIS believes that stolen information will still be used to commit cyber-dependent extortion in 2026 onwards. The sum of stolen information made available on the internet *highly likely* presents a cumulative threat. The NCIS is aware that cybercriminals currently possess large and constantly growing volumes of sensitive information originating from data thefts.

Criminals have thus far not been able to process or exploit the accumulated data to any substantial extent. It is, however, *likely* that AI systems introduce new opportunities to exploit these data for criminal purposes. If cybercriminals, through the use of AI systems, are able to exploit these data to commit crime, it is *highly likely* that vast volumes of data will be given renewed value in the eyes of criminals.

In last year's report, it was assessed as *likely* that cybercriminals' influence on physical processes would bring about production stoppages at large costs to Norwegian OT dependent organisations in 2025. The assessment proved right in the past year, and remains just as relevant today. It is therefore considered *likely* that Norwegian OT dependent organisations will become targets of such influence in 2026. Furthermore, it remains *likely* that the consequences of successful cyberattacks against OT dependent organisations will ripple across the supply chain, and there is consequently also *an even chance* that they will cause disruption to physical processes linked to critical infrastructure or vital services and utilities.

National trends and developments

Cyber-enabled sexual crime

In 2025 the police recorded 3212 cases involving sexual crime against children,[56] down from 3395 cases in 2024. 36% of the cases, or roughly one third, were reported over a year after the crime allegedly took place. The chapter of the Norwegian Penal Code describing the different types of sexual offences is technology neutral, and the statistics consequently fail to tell us what proportion of these offences is cyber-enabled.

An estimate of cyber-enabled sexual crime must therefore be based on the modi operandi, and requires that this has been manually recorded in each case. In 2025, a digital MO was specified in slightly under 1900 of the cases involving sexual crime. These can be assumed to be cyber-enabled crimes.

In addition, the NCIS received and transmitted a total of 3001 NCMEC tip-offs to the local police districts, all of them concerning online child sexual exploitation. This shows that the number of reported cases for a specific digital MO does not give an accurate picture of the extent of cyber-enabled sexual crime. The reasons why some tip-offs are not included in the reported-crime statistics may be that a low priority within the case portfolio of the local police district causes long case processing times, that no criminal investigation has been opened or that the matter has been handled outside of the criminal justice system. This tentative explanation is directly linked to the resource situation of the police districts.[57] Matters that tend to be given low priority are offences provided for in section 311 of the Norwegian Penal Code: depiction of sexual abuse of children or depiction which sexualises children (so-called 311 cases). However, there are a number of examples of investigations that first appeared to be straight-forward 311 cases, but where extremely serious child sexual abuse was later uncovered. This goes to show the potential consequences of a lack of resources. See page 19. for more about the causes of dark figures that have a relevance to recorded cyber-enabled sexual crimes.

In 2025, 1479 "311 cases" were recorded, the majority of them with a recorded digital MO. The numbers were very similar in 2024, with 1530 recorded criminal cases. As regards synthetic child sexual abuse material, the NCIS received 90[58]

56 2780 children were recorded as victims in these cases, all of them between the ages of 0 and 17 at the time of the offence.

57 Local police districts have for many years reported a shortage of staff to investigate an overwhelming number of sexual offence cases. When a small police district is investigating several large, complex cases, this impacts the district's ability to handle the remaining case load.

58 The tip-offs originated from Open AI and X.AI (Grok).

tip-offs in 2025 about Norwegian citizens who had been involved with synthetic child sexual abuse material, up from 15[59] in 2024. A significant increase has also been recorded internationally. In the first quarter of 2025, NCMEC received 33,100 alerts about synthetic material, compared to 67,000 in the whole of 2024 and 4700 in 2023. In 2025, another change was recorded in the production of synthetic child sexual abuse material. More actors who previously produced high-quality synthetic child sexual abuse images have now turned their attention to the production of synthetic child sexual abuse videos. This has led to a stagnation or fall in the quality of still images, as other, less experienced or less competent actors have taken over the production.

2025 saw an increase in reports to the Norwegian police of cases with indications of or links to *extreme, violent online communities*. The first known case in Norway was recorded in 2022, and the prevalence remained stable until 2025. Information about cases involving Norwegian actors and victims were received as tip-offs through NCMEC or other police channels and from foreign criminal investigations. Cases received through NCMEC reports had in many cases been uncovered in connection with a sexual offence against a child. What first appears to be a sexual offence case may have more to it than initially meets the eye, and in some cases additional offences have been detected through further investigation. The motive is not necessarily sexual; in many cases acts such as sexual extortion are merely a means to control the victim and coerce them into committing other serious acts.

By September 2025, a two-digit number of criminal cases bearing the hallmarks of the "cult" phenomenon had been recorded in Norway. Both the perpetrators and victims in these cases include Norwegian minors. The victims recruited into or pressured to join these groups are often vulnerable young people, primarily girls. Observations from Norway show that both the initial contact and further communication take place on social media and gaming platforms and end-to-end encrypted messaging platforms. However, open mental health support groups have also been exploited to approach victims.

In September 2025, the NCIS published a press release and posted information about the cult phenomenon on the politiet.no[60] website and in the NCIS' social media channels. The phenomenon has also caught the attention of mainstream media.

Reports of sextortion remained at a stable high level in Norway throughout 2025. This is consistent with last year's assessment. No

59 The tip-offs originated from Open AI. X.AI (Grok) did not make any reports to NCMEC in 2024.

60 The police. (2025). *Ekstreme nettsamfunn*. https://www.politiet.no/rad/trygg-nettbruk/ekstreme-nettsamfunn

significant changes have been recorded in actors, victims, methods or enablers[61]. However, a marginal increase has been recorded in the number of Norwegian perpetrators and Norwegian female victims under the age of 18.

Partial assessments

In last year's report, the risk of synthetic child sexual abuse videos of realistic quality occurring in 2025 was assessed as *likely*. Despite the NCIS not having recorded any such videos, there is *an even chance* that they exist. It is *likely* that realistic synthetic child sexual abuse videos will be in circulation in 2026. This assessment is substantiated by the fact that actors with the skill sets required to create true-to-life synthetic child sexual abuse images devoted considerable amounts of time to the production of videos in 2025. Based on the growing global trend, it is further *likely* that Norwegian actors' involvement with synthetic child sexual abuse images will increase in 2026.

It is *highly likely* that 2026 will see an increase in cases linked to extreme, violent online communities and that Norwegian children and adolescents will be amongst the perpetrators as well as the victims. This is substantiated by the stably low incidence of the phenomenon in Norway during 2022–2024 followed by an increase in 2025, similar to that in many other countries. The increase is *likely* due in part to the increased knowledge and awareness of the phenomenon. It is also *likely* that more Norwegian perpetrators and victims will continue to commit serious acts in the future, exposing themselves and/or others to grave danger.

It is *highly likely* that the incidence of financially motivated sexual extortion, or "sextortion", will remain stably high in 2026. This is supported by the reporting frequency in 2025. It is *highly likely* that many of the victims of this type of crime will continue to be boys under 18, and there is also *an even chance* that Norwegian boys in 2026 will fall victim to the trend observed in other countries, whereby depictions of the abuse are being sold on as CSAM.

61 In last year's cybercrime report, the term "enabler" was used to refer to technological tools and digital infrastructure. In this year's report, physical tools have also been included in this concept.

> The motive is not necessarily sexual; in many cases acts such as sexual extortion are merely a means to control the victim and coerce them into committing other serious acts.

Photo: Shutterstock

Cyber-dependent crime

In 2025 the police recorded 349 criminal cases involving *computer intrusion*. Individuals make up a large percentage of the victims in these cases. The number of cases is up by 104 from the previous year, and by 98 from 2023. The increase in 2025 may be due to a number of different factors, including an actual higher incidence of computer intrusions and a higher propensity among victims to report these crimes, but also to organisational factors, resources and priorities within the police. Despite the considerable increase from 2024 to 2025 compared to the 2023 numbers, the increase is not considered to be a significant deviation from the normal state.

The NCIS noted around 17 different iterations of ransomware linked to known *RaaS operations*[62] used in cyberattacks against Norwegian small and medium-sized enterprises (SMEs)[63] in 2025. The NCIS does not have information about any large enterprises being targeted in the same period. The types of ransomware used are well-known to the police as they are established products in the international RaaS ecosystem and have been used to target victims across the globe.

In April and May 2025, two Norwegian businesses were targeted by cyberattacks from the same hacktivist group. A common feature of the attacks was that the victims were subject to a computer intrusion enabling the threat actor to manipulate the business' OT systems. These attacks were the first examples of hacktivists targeting Norwegian businesses with computer intrusions. Hacktivists using computer intrusion as a form of attack had previously only been observed in other countries. As such, the attacks represent a deviation from the normal state in Norway, where hacktivists usually target their victims with denial of service attacks. Although the damage caused by cyberattacks from hacktivists has thus far been limited, this development shows that hacktivists hone their tools and methods to achieve the desired effect. Hacktivism consequently represents both a crime problem and a security policy instrument (see page 75), with overlapping grey areas between freedom of expression, illegal influence and degrees of government support.

62 Examples of known RaaS operations include Akira, Qilin, Lynx, LockBit, 8base and DragonForce.

63 Small and medium-sized enterprises (SMEs) are businesses with fewer than 250 employees, an annual turnover not exceeding EUR 50 million and/or a balance sheet total not exceeding EUR 43 million. Source: *EØS-tillegget til Den europeiske unions tidende*. (04.04.2019). EØS-tillegget til Den europeiske unions tidende, no. 28/1133. p. 1. https://www.regjeringen.no/contentassets/1bdef920d6cc4245b2e09a5902cb4374/vedlegg1.pdf

Partial assessments

Based on current trends, it is *likely* that the increase in received complaints for cyber-dependent crime will continue in 2026. Part of the increase will be due to an increased propensity to report these crimes, but it is nevertheless *likely* that there will be a real increase in cyber-dependent crime in Norway. This is mainly due to increased commercialisation of crime and the fact that technological innovation is, in itself, a global driver of cybercrime.

Hacktivist groups are *likely* to strengthen their operational capacities through digital recruitment, sharing of experiences and the use of technological tools. Better access to tools and a willingness to cooperate across groups will *likely* boost capacity, improve capability[64] for target selection and increase the impact of campaigns.

Although hacktivist groups today have limited ability to carry out attacks against OT systems, it is *likely* that they in the future will be able to inflict physical damage or destruction. This as a result of sharing of expertise and malware and partnerships with more advanced threat actors.

64 The term "capacities" refers to the quantifiable features and assets of criminals. Examples include physical and mental stamina, the number of individuals in a group and digital assets. Together, a group's capacities and their ability to exploit them make up the group's capabilities.

Technological advances have redefined the term *social inclusion*. Social media, online forums and communication platforms, games and other internet based entertainment have created new arenas for social interaction between people. Persons who were previously cut off from social meeting places can now get together with like-minded people in these new arenas.

Photo: Shutterstock

The cybercriminal ecosystem

This section seeks to outline the mechanisms and dynamics of the criminal ecosystem by looking at previous reports and enriching the analyses with new data. It will introduce new and revised models of the cybercriminal ecosystem and is intended as support for future analysis efforts.

Each year, around 280 to 300 million people connect to the internet for the first time, many of them in countries struggling with a high poverty rate, a low education rate and weak government control.[65] High-speed internet can be a catalyst for economic growth, boost education and health systems, contribute to social inclusion and play an important role in national emergency preparedness. But this evolution also means that more criminal actors migrate or move part of their activity to the digital space. Countries that recently embarked on the journey towards digitalisation and just gained access to faster and cheaper internet, are experiencing sociological and economic challenges that have previously contributed to the emergence of geographical hot-spots for cybercrime in other countries[66].

Another large group connecting to the internet for the first time each year are children and adolescents. The current generation is growing up with social media, internet gaming and artificial intelligence as everyday phenomena: an indissociable part of their augmented reality. But whilst children and adolescents may have advanced technical skills from an early age, they also tend to be easily influenced and have an underdeveloped understanding of risk and poor consequential thinking. When children and adolescents are allowed to roam freely online and communicate with whoever they

65 ITU & UNESCO. (2024). *The State of Broadband: Leveraging AI for Universal Connectivity, Part One – June 2024*. Broadband Commision for sustainable development. https://www.unesco.org/en/articles/state-broadband-2024

66 E.g. Russia, Ukraine, Romania, Nigeria, India, China and countries in South-East Asia.

When children and adolescents are allowed to roam freely online and communicate with whoever they like without any kind of supervision or parental guidance, the risk increases that they either become victims of crime or are recruited or drawn into criminal activities, be it intentionally or inadvertently.

Photo: Shutterstock

like without any kind of supervision or parental guidance, the risk increases that they either become victims of crime or are recruited or drawn into criminal activities, be it intentionally or inadvertently.

With the increase in online users comes an increase in cybercriminal actors incessantly developing new methods and approaches to exploiting technology in order to harm Norwegian values.

Some cybercriminal networks have a hierarchical structure with clear roles and chains of command, whereas others are loosely organised with temporary, transactional alliances. A vast, fragmented crime picture with many floating elements combined with fast-paced change, makes it hard to draw up a precise description of the full ecosystem. In a wider cybercriminal ecosystem with no fixed structure or hierarchy, the actual collaboration mechanisms, i.e. the mechanisms affecting how criminals interact and work together, are key to understanding prevailing trends.

Figure 3 is a diagram of the *ontology*[67] of cybercrime with descriptions of some of its basic mechanisms. Section B (pale blue) represents the actual crime and illustrates how a criminal actor moves through an attack phase and its intermediate objectives towards the final goal in order to harm a victim.

To succeed with the attack, the actor must carry out supporting activities[68] and exploit the victim's vulnerabilities, as illustrated in section A (pale green).

Section C (pink) illustrates how the actors rely on support factors: enablers[69], facilitators[70] and partners[71]. Actors must also relate to adversaries, including government authorities, private companies, research institutes and rival criminal actors.

The diagram also includes basic drivers and triggers that influence crime, as represented in section D (pale yellow). Some examples of triggers are war and conflict, sporting events, referendums, award ceremonies and other events that may trigger cybercrime.

The model is focused around crime committed against individuals, organisations or infrastructure, but criminal activity can take place within all the red boxes. The dynamics between the red boxes constitute the foundation of the cybercriminal ecosystem.

---

67 Ontology is the philosophical study of existence. Source: Bøhn, E. D. (22.02.2025). *Ontologi*. Store norske leksikon. https://snl.no/ontologi

68 Often referred to as the *kill chain*.

69 E.g. digital infrastructure, tools and meeting points.

70 E.g. initial access brokers, money launderers and criminal platform providers.

71 E.g. other criminal actors working towards a shared goal.

Actor gallery

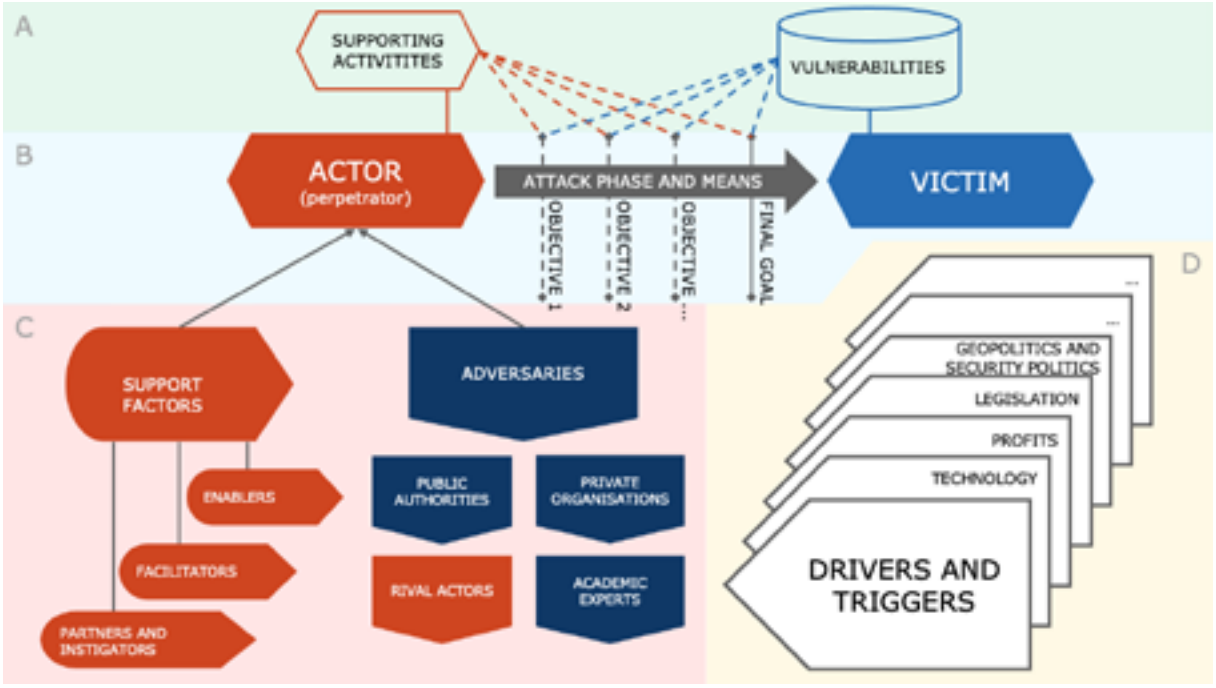


Figure 3: *The ontology of cybercrime.* The model shows how a crime (B) is carried out in an attack phase through which a criminal actor seeks to meet a set of intermediate objectives towards a final goal. In order to succeed, the actor must exploit vulnerabilities and carry out supporting activities (A). The actor is often assisted by enablers and partners, but also countered by authorities and other actors (C). Crime is also affected by drivers and triggers such as war, conflict or major events (D). The model shows a dynamic ecosystem in which all parts are interconnected. The model is developed by the NCIS, inspired by A. J. Greimas[72] and builds on the "Eleven cybercrime drivers" model presented in *Cybercrime 2023*[73].

72 Greimas, A. J. (1984). *Structural semantics: An attempt at a method.* Etera. https://www.etera.ee/zoom/50614/view?page=267&p=separate&tool=info&view=0,0,2049,3458.

73 NCIS. (2023). *Cybercrime 2023*. pp. 14–32.

The term "actor" has been used, by police and others, to describe everything from individuals and groups to digital tools and malware, and the terms *roles* and *profiles* are frequently confused. This is unfortunate, and can for example lead to, on the one hand, CaaS and, on the other, individuals or groups being referred to collectively as one actor.[74] This challenges the police's and private security companies' ability to keep track of the gallery of criminal actors and, consequently, to assess the threat presented by various individuals and groups.

The model in Figure 4 has been named the *ARPA framework* and is intended to systematise the terminology by describing the structure of the actor gallery on four levels. The model is based on the *iceberg* model from *Cybercrime 2025*[75], which shows the connection between the actors' underlying and more constant motivations and their visible actions and roles. The model takes into account the heterogeneity of cybercrime[76] by emphasising which levels are dynamic and which are more static. The greyscale is used to show which categories are fleeting and which are more stable: white background indicates fleeting elements, and darker backgrounds indicates a higher degree of stability.

At the end of the day, cybercrime is about *people*: the drivers of crime are human interests. The model can be used as a check list in investigations to assess whether the different levels of actors have been uncovered. A comprehensive overview of the actors can be key in uncovering any use of hybrid means by state actors, and it may also help point out any changes in dynamics between the various roles and profiles.

The model shows the four levels of the actor gallery. The levels show the actors committing the crime (*actor*), their motivations (*profile*), their role in the ecosystem (*role*) and the actions or tasks they carry out (*activity*).

The top level (Actor) shows the people committing the crimes.

The next level (Profile) consists of five different profiles[77] as well as a group of uncategorised actors. The profiles are unchanged from last year's cybercrime report and will be described in more detail later in this section.

The third level (Role) is split into two groups: *facilitators* and *perpetrators*. In contrast to

74 The name of a criminal service is often used to refer to otherwise unknown or unnamed individuals or groups.

75 NCIS. (2025). *Cybercrime 2025*. p 13.

76 New constellations emerge and change fast.

77 Terrorists are not included in this report as terrorist activities fall outside the remit of the NCIS.

> Cybercrime is ultimately about people and driven by human interests.

Photo: Shutterstock

facilitators, perpetrators are those who actually commit the crimes against individuals or organisations. The same actor can be a facilitator or a perpetrator depending on the situation.

At the bottom level (Activity) are a number of boxes representing various situations (referred to as "areas of activity"). Each box shows the breakdown of a situation into observed activities, and consequently says something about the organisation of different roles in different situations. The list of elements in each box does not have to be exhaustive to support the analysis, any available knowledge and information is helpful. The framework helps analysts understand the situation and contextualise the threat, and it can also help increase awareness when assessing various criminal activities in the digital space. The framework can also be used in other contexts. Based on the organisation of various roles observed, we have provided four examples of situations with typical associated activities.

The right hand side of the model is a list of *enablers* comprising technological tools, digital infrastructure and physical tools.

The following is an example of how the model can be put to use and its relevance for understanding the links between various actors in different areas of crime.

(A) Child sexual abuse
(R) Cult member[78]
(P) Uncategorised actor
(A) John Doe

In this case, an assumption about the actor's profile based on actions (activity) alone might lead to an erroneous interpretation of the motivation for their actions. Based on such an assumption the actor, John Doe, is likely to be categorised as a sexual offender rather than an uncategorised actor whose motivations are not sexual. The example illustrates why it is important to identify all actor levels to make a precise assessment of the threat.

In cases where a single actor is associated with multiple simultaneous activities, roles or profiles (for example multicriminals or actors operating in grey areas), it may for example look like this:

Multicriminal:
(A) Recruitment of perpetrators
(R) People-smuggler; Facilitator of LDCA
(P) Profit-motivated criminal
(A) John Doe

Actor operation in grey areas:
(A) Searching for vulnerabilities
(R) Hacker
(P) Activist/terrorist
(A) Unknown

78 Read more about cult members on pages 82–85.

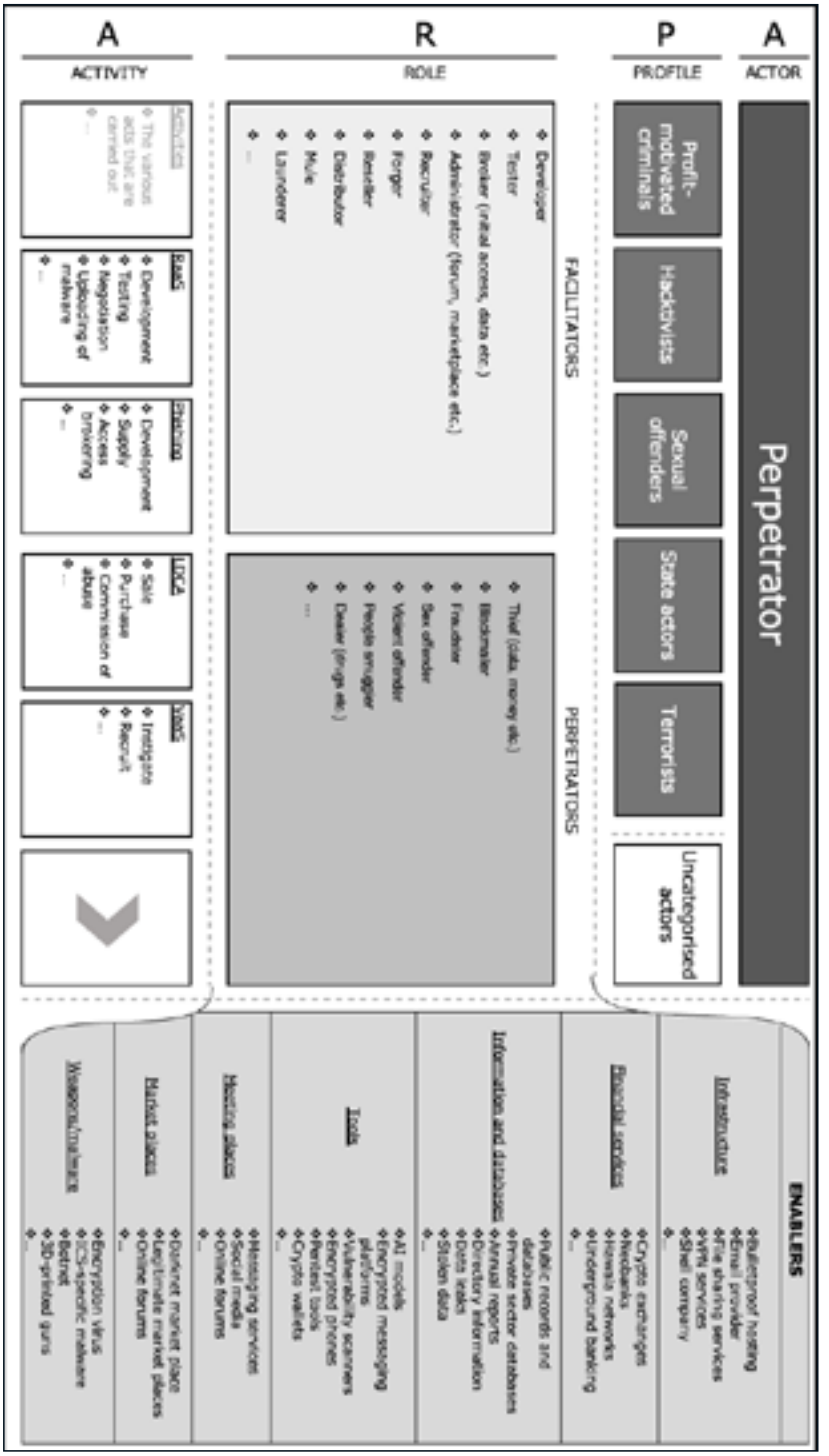


Figure 4: *The ARPA framework*. The model should be read from the bottom up, from activities to actors. The model is developed by the NCIS and inspired by the work of A. J. Greimas[78].

The *ARPA framework* helps explain the ecosystem of actors through clear definitions for each level of the diagram. The framework further maps various activities and roles (facilitators and perpetrators), providing useful decision-making support for prioritisation of cases. The NCIS invites other police services, public authorities and private-sector organisations handling a wide spectrum of threats to contribute to the continued mapping and identification of key activities and roles across different areas of crime.

Profit-motivated criminals

Commercial actors

Some traditional commercial actors may have a criminal side. Such commercial actors can have the same basic motivations as profit-motivated criminals, i.e. money and influence, but differ from the latter in that their core activity takes place within commercial enterprises that appear to meet the expectations and regulatory requirements of society.

Offences committed by commercial actors mainly consist in 1) the exploitation of temporary loopholes emerging as a consequence of technological advances or weaknesses between jurisdictions; or 2) the selling of illegal goods and services to a) maximise profits from their own core activities; or b) facilitate crime. This includes goods and services in the grey area between what is legal and illegal,[80] so-called dual-use items[81], and traditional organised crime and economic crime.[82]

Profit-motivated criminal actors exploiting commercial enterprises – such as shell companies or organisations used as fronts to launder proceeds of crime – are as a rule not included in

79 Greimas, A. J. (1984). *Structural semantics: An attempt at a method*. Etera.

80 Either because an actor deliberately exploits a legal loophole, because parts of the operation are legal whilst others are not, or because the product is legal in one context but illegal in another. Examples include AI models that can generate illegal content, tools to circumvent digital rights systems, drones with particular specifications and private sector intelligence and security companies who employ excessive means.

81 Dual-use items are goods that, although intended for civil use, can also be used for military purposes. The term is here used in a wider meaning to include criminal applications.

82 Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim). (2022). *Threat assessment 2022*. p. 61. https://www.okokrim.no/getfile.php/5017571.2528.q7zikqspuaaqqs/%C3%98kokrim+trusselvurdering+2022.pdf

this category. However, the distinctions are not always clear-cut.[83] In some countries, it is not unusual that public officers or private-sector employees also hold positions within criminal organisations and juggle between roles. This contributes to blurring the lines between commercial actors and state actors and other profit-motivated criminals.

Some examples of roles that may be assigned to commercial actors are surveillance services[84], negotiations in connection with ransomware attacks (RaaS)[85] and the provision of digital infrastructure[86] or services[87] facilitating or concealing crime.

Criminals engaging in extortion

Cyber-dependent extortion can take place in a number of ways and by different constellations. Since 2010, the use of what is known as a *RaaS kit*[88], including various supporting services supplied by a RaaS network, has become the extortionists' preferred method. In the past 15 years, this has developed into one of the most prolific business models for cyber-dependent extortion.

Although most RaaS networks are still centred around the use of malware with an encryption feature, not all RaaS networks today rely on encryption. Over the past five years, it has become increasingly common for cybercriminals to commit extortion based on data theft and threats to publish the victim organisation's data without encryption. In such cases, the term "ransomware-as-a-service" (RaaS) can be somewhat inaccurate and misleading as no malware with encryption features is involved. The term "extortion-as-a-service" (EaaS) has been coined to include traditional RaaS net-

83 Ibid. p. 61.

84 Providers of high-tech cyberweapons such as private surveillance and commercial spyware that are subject to licencing but not to export control or sanctions.

85 Providers of negotiation services who enter into covert deals or share proceeds of crime with ransomware actors, referred to as ransomware/extortion negotiation and cyber extortion incident response providers.

86 E.g. bulletproof hosting, and VPN and proxy services.

87 E.g. IP stressers (also known as *DDoS-for-hire*), file sharing services, end-to-end encrypted messaging platforms and email providers.

88 A RaaS kit, or RaaS panel, is a software application with a variety of features. (RaaS is an abbreviation for Ransomware-as-a-Service.) RaaS kits are rented out to criminals of all skill-levels wanting to commit cyber-dependent extortion, for a share of the profit.

> Virtually anyone with access to the internet can join an EaaS network.

Photo: Shutterstock

works as well as criminal constellations engaging in other forms of cyber-dependent extortion but still operating within a crime-as-a-service (CaaS) context. The key point is that the software and its uses are fleeting and changing, but the people behind the actions and their intentions remain constant over time.

Almost anyone with access to the internet can join an EaaS network. The fact that two or more criminals are part of the same EaaS network or use the same ransomware, does not automatically mean that they constitute a defined cybercriminal group.[89] The use of a specific variety of RaaS says, in itself, very little about the individual criminal's capabilities or motivations. The ability of affiliates[90] to juggle between several types of EaaS presents an additional challenge to the police in that it makes it harder to recognise perpetrators across cyberattacks, types of malware and groupings or networks.

In connection with an investigation into several computer intrusions in Norway, the NCIS found that the perpetrator had used four different types of ransomware and, possibly, also a fifth one through RaaS. The perpetrator has been linked to cyberattacks against more than 130 organisations outside Norway and has extorted ransom payments totalling almost NOK 50 million (around EUR 4.5 million) from the victims. The example shows that a single criminal can be affiliated with and simultaneously use a number of different ransomware applications.

The NCIS has found traditional RaaS groupings to be open or closed to varying degrees. Past analyses of the ransomware grouping *HIVE* found that it consisted of a centrally operated core group with a restrictive approach to the distribution of tasks, who selectively recruited new personnel into the core

89 A cybercriminal group is a collection of individuals who collaborate to achieve a common goal through the commission of cybercrime.

90 An affiliate is a person who has a business-like relationship to a RaaS or EaaS grouping and who makes use of ransomware-as-a-service.

group. The group had a discreet approach to recruiting affiliates on cybercrime forums. In comparison, groups such as *Lockbit* gradually opened up their profile and made the Lockbit ransomware accessible to anyone interested in using it, against payment. As a consequence, Lockbit attracted inexperienced affiliates who made operational errors. This further contributed to weakening Lockbit's professional profile and reputation.

The fragmentation of the EaaS ecosystem has increased the competition to attract new affiliates. Some EaaS networks aiming to maximise recruitment and turnover, market themselves as better than their competitors. A central part of the marketing consists of harming large high-profile organisations to create maximum buzz. Many RaaS groupings have a clear media profile and make statements to traditional media outlets. The rationale for this trend is the idea that through building a reputation as an infamous ransomware, RaaS groupings will increase their negotiation power towards their victims. There are also examples of RaaS groupings who have created an image of themselves as a capable actor by suggesting that they were behind attacks on important organisations, without the claims ever being proved or disproved. Such rhetoric and promotion of merits may put additional pressure on the victim in a negotiation situation, but also help attract new talent (affiliates) to the core group. Additionally, there have been reports of an influx of younger criminals with a higher propensity for risk-taking, high ambitions and eagerness to attract the attention of the media. This has given rise to a number of contested incidents and to new constellations and loose federations across the EaaS ecosystem.

Based on investigations and international police cooperation, the NCIS have mapped more than 400 criminals with ties to the cybercriminal ecosystem. This work has mainly been informed by investigations into various combinations of computer intrusions, data theft, encryption and extortion, in Norway and abroad. The majority of the actors mapped are in some way linked to one or more varieties of RaaS. Persons with other and more secondary roles in the cybercriminal ecosystem have also been mapped.

By the end of 2025, this mapping effort had led to the identification of a significant number of cybercriminals, some of whom have also been circulated as wanted internationally. The work has yielded valuable insights into the mechanisms and dynamics of the cybercriminal ecosystem.

The criminals identified are exclusively male, most of them between 20 and 40 years of age, and most of them originally Russian or Ukrainian, although a number of nationalities are represented. A common denominator is that most of them have Russian as their language of choice. Some of them have a formal IT-related qualification, but most seem to lack

> Based on investigative efforts and international police co-operation, the NCIS has mapped out more than 400 criminals with varying links to the cyber-criminal ecosystem.

Photo: Shutterstock

formal education. There are indications that the oldest members of the identified group have been involved in various forms of cyber-dependent crime for a number of years, and that they first started with RaaS around 2009, when this crime type gained momentum following the emergence of cryptocurrency.

Criminals engaging in extortion by ransomware watch keenly for any new measures taken by authorities or the security sector to counteract and fight cybercrime. They are also very much aware of how specific EaaS groupings are referred to and assessed in public threat assessments. This can for example manifest itself in the sharing of and discussions regarding various threat assessment, news reports of police interventions and measures targeting cybercriminals.

The NCIS has seen some examples of cybercriminals deciding to move on to other kinds of RaaS when they feel that one type attracts too much attention from the authorities. This, however, goes against the international trend observed in recent years whereby some EaaS networks seem to work actively to draw attention to their own RaaS networks.

Partial assessments
Criminal actors committing cyber-dependent extortion are mainly driven by a desire for profit. It is the NCIS' understanding that profit-motivated cybercriminals will continue to develop their approach and adapt to countermeasures in their chase for financial gain, in 2026 and beyond. To commit cyber-dependent extortion, criminal actors rely on a means of coercion, either stolen data or encryption of the organisations' systems. This is *unlikely* to change in 2026.

Profit-motivated sexual criminals
Profit-motivated sexual offenders are actors who commit sexual crimes against children, but whose motive is financial gain. The NCIS has identified three main categories of profit-motivated sexual offenders: (1) Sellers of live distant child abuse (LDCA), (2) extortionists; and (3) actors who offer child sexual abuse material for sale. All of them commit sexual offences, but in different ways.

Before the advent of the digital space, there was no LDCA. Technological advances have led to children in high-risk countries being sold and subjected to both contact and non-contact sexual abuse. LDCA sellers are generally women from the Philippines with young children of their own. Some are facilitators who organise

and share live distance child abuse of their own or other people's children, others commit the physical sexual abuse. In many cases they take on a combined role of facilitator and abuser.[91] As described on page 39 in the section about the normal state, LDCA is sold to sexually motivated Norwegian men.

No cases have been recorded of Norwegian actors selling LDCA of Norwegian children, neither to Norwegian nor foreign buyers. The NCIS is, however, aware that Norwegian offenders have sold sexualised material of their own children to sexually motivated actors. In addition, the advent of cyberspace has paved the way for a market where children and adolescents sell self-generated sexualised material of themselves and others to sexually motivated actors. The children may think of it as easy money without being aware of the potential future consequences and the risk it entails. The images may exist forever online, where sexually motivated actors can continue to share them, and the children may sell images and videos to actors with a serious propensity for violence, thereby putting themselves in great danger.

As documented in last year's cybercrime report, the majority of profit-motivated sexual offenders who commit sextortion against Norwegian children are based in the Philippines, Nigeria and the Ivory Coast. They are more loosely organised than previously thought, and the type of crime they commit is relatively simple to carry out and associated with a low risk of detection and prosecution.[92] As previously mentioned, no significant changes to the normal state have been recorded, although there has been a marginal increase in the number of Norwegian extortionists and the number of young girls who fall victim to these crimes.

In contrast to the two aforementioned types of crime, the sale of CSAM does not harm the child directly when the crime is committed, but can nonetheless perpetuate the harm caused to the victim. The NCIS is aware that Norwegian sexual offenders buy CSAM from foreign and national profit-motivated actors, and trading of both authentic and synthetic abuse material has been recorded. However, as mentioned in the description of the normal state, actors involved with CSAM usually exchange such photos and videos with their peers without any form of payment. It is uncertain whether, or to what extent, some of the Norwegian actors might be both sexually motivated and profit-motivated.

Cyberspace has expanded the arena on

91 NCIS. (2023). *Live distance child abuse (LDCA)*. p. 5. https://www.politiet.no/globalassets/tall-og-fakta/seksuelle-overgrep-mot-barn/direkteoverforte-bestillingsovergrep-dobo.pdf

92 NCIS. (2025). *Cybercrime 2025*. p 7.

which profit-motivated actors, including sexual offenders, can operate. New possibilities arise, the group of actors expand, and the methods and procedures used by criminals are constantly evolving, as witnessed by the NCIS. The umbrella term "crime-as-a-service" comprises a vast repertoire of criminal services offered for sale. Last year, the NCIS reported that recent developments within the field of AI may lead to automation and upscaling of the processes used to approach and groom victims.[93] Perhaps grooming-as-a-service will be included in the portfolio of services available on the market in the years to come.

Partial assessments

One of the strongest drivers of cybercrime is the desire for profit, and the actors are adaptable in their methods. Some child sexual abuse is committed for financial gain. Sexual motivations are a strong driving force that can be exploited by profit-motivated actors to make money. Crime can spread in an unlimited number or directions, and it is *likely* that profit-motivated actors will find new ways to profit from various types of sexual crimes. There is *an even chance* that this may take the form of crime-as-a-service.

The relationship between criminals and state actors

In light of the tense global geopolitical environment and the current national Total Defence Year in Norway, the NCIS has decided to study the complex situation surrounding state actors and their involvement in cybercrime. Interactions between state actors and criminals mostly take place in cyberspace.

A common characteristic of cybercrime is that the offender tends to be previously unknown to the police, and that it is through investigation that the actors behind the crimes are exposed. The police therefore need insight into the involvement of state actors in the cybercriminal ecosystem so that the investigation can be transferred to other agencies should the scope of the investigation change over time.

Rivalry between superpowers and international conflicts are blurring the already unclear divisions between state and cybercriminal actors. This is particularly true for the divisions between state actors, hacktivists and p it-motivated cybercriminals. According to threat assessments published by Norwegian intelligence and security services for 2026,

93 NCIS. (2025). *Cybercrime 2025*. pp. 48–50.

Spectrum of state responsibility

1. **State-prohibited.** The national government will help stop the third-party attack.
2. **State-prohibited-but-inadequate.** The national government is cooperative but unable to stop the third-party attack.
3. **State-ignored.** The national government knows about the third-party attacks but is unwilling to take any official action.
4. **State-encouraged.** Third parties control and conduct the attack, but the national government encourages them as a matter of policy.
5. **State-shaped.** Third parties control and conduct the attack, but the state provides some support.
6. **State-coordinated.** The national government coordinates third-party attackers such as by "suggesting" operational details.
7. **State-ordered.** The national government directs third-party proxies to conduct the attack on its behalf.
8. **State-rogue-conducted.** Out-of-control elements of cyber forces of the national government conduct the attack.
9. **State-executed.** The national government conducts the attack using cyber forces under their direct control.
10. **State-integrated.** The national government attacks using integrated third-party proxies and government cyber forces.

To fully understand the interaction between state actors and cybercriminals, it is important to be aware that there are degrees of state links. In order to avoid any wrongful attribution to other countries, we will take Norway as an example. *Norwegian actors, Norwegian state actors, Norwegian actors with links to the state* and *pro-Norwegian actors* are possible examples. In the first category are actors originating from Norway or who hold a Norwegian passport. A *Norwegian actor* does not necessarily have ties to the Norwegian state. *Norwegian state actors* are actors representing the Norwegian government. The term *Norwegian actor with links to the state* is used when there is sufficient evidence to link the cybercriminal actor to persons within the Norwegian government. The last term is used to refer to actors who have expressed pro-Norwegian sympathies. The term *pro-Norwegian actor* does neither confirm nor deny any of the possible forms of contact with or ties to the Norwegian state.

Figure 5: *The Spectrum of State Responsibility*, Atlantic Council. Translation: NCIS.

state actors make use of criminal proxies[94] to attain various objectives.[95, 96]

States are not dependent on geographical closeness to cybercriminals to be able to use their services. A state can engage the services of criminals operating in or originating from other countries.

Cyberspace is an arena that offers very good conditions for covert activities. This complicates the efforts to expose and prosecute criminals and makes it difficult to gain insight into the interactions between cybercriminals and state actors. The framework of the Atlantic Council (*Spectrum of state responsibility*, figure 5) lists ten levels of state responsibility for cyberattacks committed by criminals. The model encompasses everything from states that contribute to stopping criminal acts (level 1) to states that execute the attack, either themselves (level 9) or through an integrated third-party (level 10). In light of the threat from state actors, as described by Norwegian intelligence and security services, it is important to be aware of this spectrum. The framework enriches the picture of the cybercrime situation and can be used to interpret matters involving cyber-dependent crime in particular.

There are various degrees of interaction and *cross-pollination*, among criminal actors and between criminal actors and state actors. The term "cross-pollination" denotes the transfer of tools, methods and malware from one actor to another without there necessarily being a cooperation.

Over the past few years, a number of actual or strongly suspected instances of state involvement in cybercriminal operations or attacks have been uncovered in Norway and other European countries. Cyberattacks have been on

94 Criminal proxies are persons or organisations with no formal links to intelligence or security services or other government agencies, who, knowingly or not, commit crime on behalf of or in support of governments. The activities may be politically, ideologically or financially motivated. Source: Norwegian Police Security Service. (2025). *Nasjonal Trusselvurdering 2025*. p. 12. https://www.pst.no/globalassets/2025/nasjonal-trusselvurdering-2025/nasjonal-trusselvurdering-2025_no_web.pdf

95 Norwegian Police Security Service. (2026). *Nasjonal trusselvurdering 2026.* pp. 12–13, 16–18, 22–23. https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-pa-norsk/Fokus2026%20-%20N0%20-%20Utskriftsvennlig%20v4.pdf

96 Norwegian Intelligence Service (2026). *Fokus.* pp. 27–29. https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-pa-norsk/Fokus2026%20-%20N0%20-%20Utskriftsvennlig%20v4.pdf

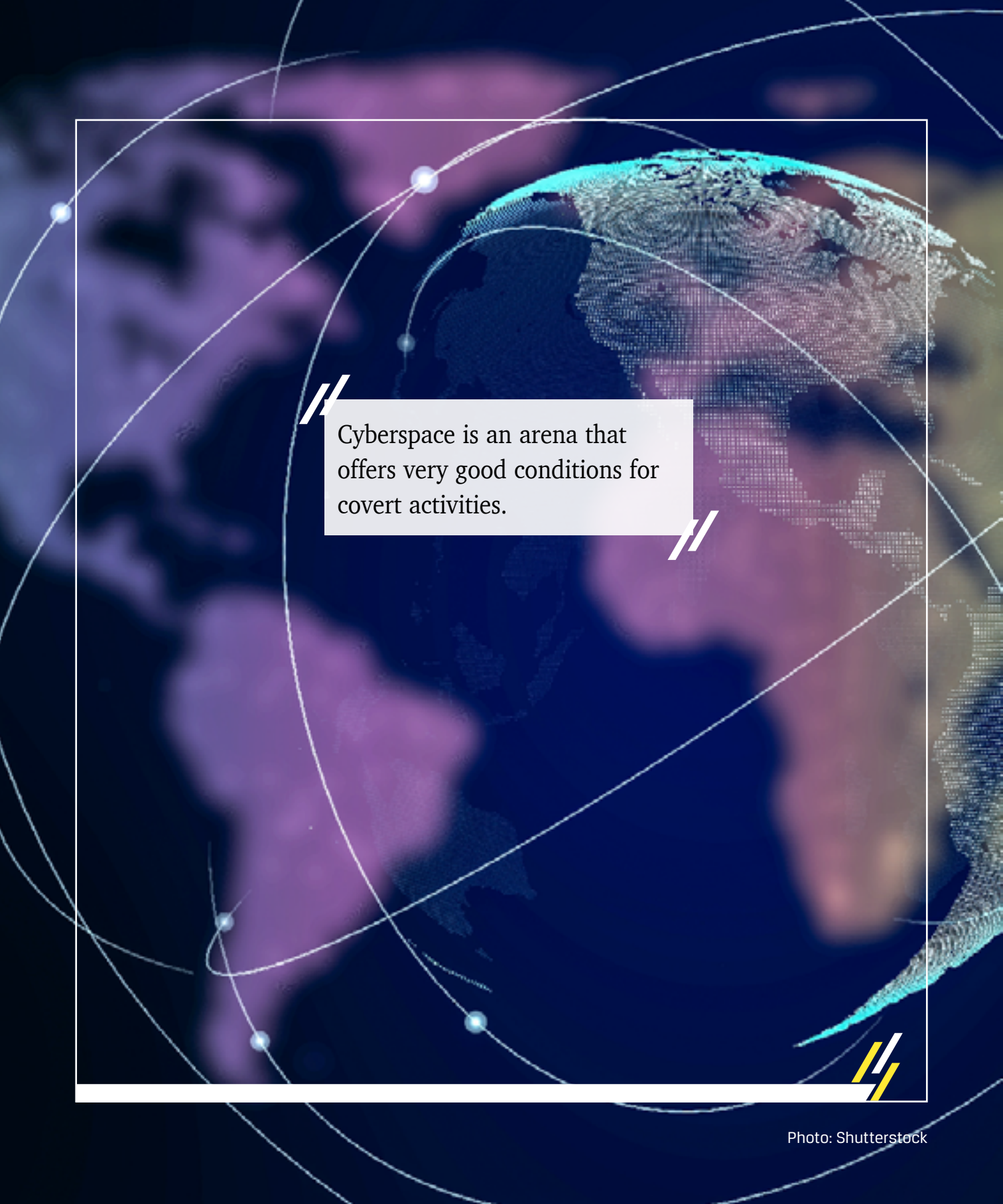


Photo: Shutterstock

the rise in the past few years in parts of Europe, and the motivations behind many of these attacks are assessed as a combination of strategic[97] and financial. Norwegian industry sector and public sector organisations have also regularly been targeted. Some of the attacks carried out in the past few years have targeted ports and gas terminals, energy and communications.

Cybercriminals are to a varying degree willing to collaborate with or operate on behalf of a state. This willingness may change over time. For example, what started as a voluntary cooperation may evolve into a more coercive relationship in which one of the parties holds information or means of coercion that make it difficult for the other party to withdraw from the cooperation.

The discussion in this section substantiates the claims from Norwegian intelligence and security services that criminal proxies are part of the portfolio of means used by state actors.[98] This becomes especially clear in cyberspace where, in particular, cyber-dependent crime is equally suited to supporting criminal motives and state objectives. It is important to understand figure 5, which shows the spectrum of state-involvement in cybercrime, to be able to interpret events, understand contexts and connections and, in doing so, improve the police's ability to detect and alert to discrepancies and limit their consequences to the greatest extent possible.

97 In order to obtain information about civil and military technology. Source: Norwegian Intelligence Service (2025). *Fokus.* p. 14 https://www.regjeringen.no/contentassets/6290dec36c374ee191e5c7dbba18a258/fokus2025-no-weboppslag-v3.pdf

98 The limits between digital and physical threats can be hard to define. This landscape also includes so-called complex or hybrid threats. Hybrid measures means that state actors that want to harm other states in other ways than by armed conflict, use a variety of means and methods to support their strategic aims. Examples are covert influence operations and the spreading of disinformation seeking to destabilise democracies and weaken the population's trust in key institutions. Thus, authoritarian regimes can seek to create chaos or influence political decisions in other countries to their own benefit. Source: Parliamentary White Paper no. 13 (2024–2025). *Forebygging av ekstremisme: Trygghet, tillit, samarbeid og demokratisk motstandskraft.* Ministry of Culture and Equality. https://www.regjeringen.no/no/dokumenter/meld.-st.-13-20242025/id3092713/?ch=3

> Even though the damage so far has been limited, these developments show that hacktivists adapt their methods and tools to gain greater impact.

Photo: Shutterstock

Hacktivists

Hacktivism is a hybrid between politically or ideologically motivated activism and cybercrime and constitutes a persistent threat to Norwegian values and interests. It is a wider concept than denial-of-service attacks and also includes data theft, data leaks and distribution of stolen data as well as other politically or ideologically motivated digital crimes.

Some groups operate in the grey area between activism and profit-motivated crime, where economic profit can be used to finance hacktivism. This is a form of attack, predominantly denial-of-service attacks, used to generate attention, create unrest, weaken trust in public institutions or influence public opinion.

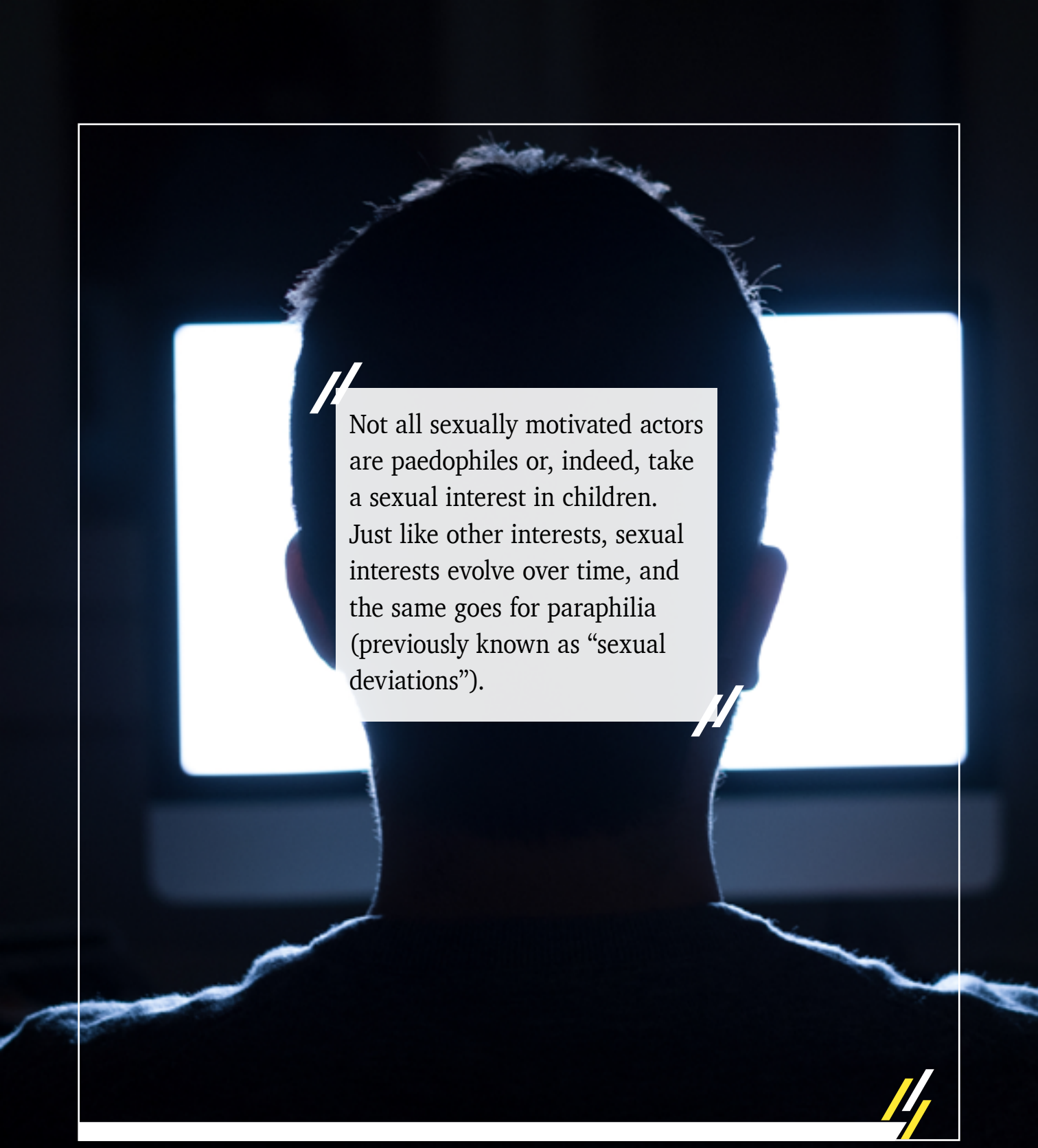
In Norway, pro-Russian groups have amongst other things carried out denial-of-service attacks and made unauthorised changes to industrial control systems. One incident in Bremanger, in which the control system of a dam was compromised and 500 litres of water was released every second for four hours, illustrates how such actors can have the ability to harm critical infrastructure. Clear links have also been found between the Russian government and cybercriminals carrying out cyberattacks to gather information about Norwegian technology and weapons.

Even though the damage so far has been limited, these developments show that hacktivists adapt their methods and tools to gain greater impact. The phenomenon consequently has the dual characteristics of a crime problem and a security policy instrument, with overlapping grey areas between freedom of expression, illegal influence and degrees of government support.

Known instances of personal attacks on publicly elected politicians, include pornographic deepfakes of the Italian prime minister Giorgia Meloni and UK politicians Priti Patel and Penny Mordaunt. In 2022, the Pro-Russia hacker group *Killnet* manipulated a photo of the then Norwegian Minister of Foreign Affairs Anniken Huitfeldt and launched the campaign "Good morning Norway All squads at battle" which included DoS attacks directed at Norwegian hospitals and government web portals.

Sexually-motivated sexual offenders

As described in the section regarding the normal state of cyber-enabled sexual crime against children, technology has become an integral part of this area of crime. It is important to understand that this is crime committed *by* people *against* people, and that although the offences are largely committed through the use of technology, they can have vast real-world implications. A single actor can commit both cyber-enabled and contact sexual abuse, either in the form of multiple offences committed



> Not all sexually motivated actors are paedophiles or, indeed, take a sexual interest in children. Just like other interests, sexual interests evolve over time, and the same goes for paraphilia (previously known as “sexual deviations”).

Photo: Shutterstock

against the same child, or as separate offences against a number of different children. It is therefore difficult to draw a clear line between actors committing physical sexual abuse and those committing cyber-enabled abuse, as the two groups tend to overlap.

Offenders committing cyber-enabled sexual crime against children make up a large and diverse group, and a high number of Norwegian children are molested each year. The actors' motivations vary, as does the nature of the sexual crimes, and the digital platforms used to enable the crimes. Despite this and the fact that some of the perpetrators feel a degree of dissociation from the offences they commit from behind the computer screen, most of them are driven by a desire for sexual gratification, just like "traditional" sexual offenders.

Sexually motivated offenders can be found in all parts of the country, social classes and age groups, but a clear majority are male and most of them young: teenagers and men in their twenties to thirties[99]. The exception is LDCA buyers, who are also predominantly male, but of a much higher average age than those committing cyber-enabled sexual crime.[100] The majority of the recorded victims are girls, which is hardly surprising given that most recorded sexual offenders are male and the majority of the population are heterosexual.[101] Against this background, it is important to stress that some sexually motivated child sexual abusers are women. Research into women's sexual preferences for children is, however, all but non-existing; it is an area that has been largely neglected by research.

Not all sexually motivated actors are paedophiles or, indeed, take a sexual interest in children.[102] Just like other interests, sexual interests evolve over time, and the same goes

99 The police. (2024). *Politiets straffesaksbehandling 2024*. p. 60. https://www.politiet.no/globalassets/tall-og-fakta/strasak/2024/politiets-straffesaksbehandling-2024.pdf

100 NCIS. (2023). *Live distance child abuse (LDCA).* p. 6.

101 Statistics Norway (26.01.2021). *Seksuell orientering i befolkningen etter alder (18–79 år).* https://www.ssb.no/444196/seksuell-orientering-i-befolkningen-etter-alder-18-79-ar.prosent.

102 Norwegian Centre for Studies on Violence and Traumatic Stress (2023). *Digitale seksuelle overgrep mot barn og unge*. Report 3/2023 p. 44. https://www.nkvts.no//content/uploads/2024/01/NKVTS-Rapport-3-2023-Digitale-seksuelle-overgrep-mot-barn-og-unge.pdf

for *paraphilia* (previously known as "sexual deviations")[103]. In other words: what arouses a person sexually, is susceptible to change over time. The combination of watching pornography and having an orgasm strengthens the patterns of sexual arousal. Watching harmful pornography, for example depictions of street rape, may cause someone to develop a pattern of arousal to this. This is equally true for child sexual abuse material, both genuine and synthetic. As well as having a desensitising effect, exposure to pornography or CSAM may therefore increase certain sexual interests and paraphilias and cause them to develop further.[104]

Paedophilia is both a sexual orientation and a psychiatric diagnosis and considered a sexual development disorder which is either congenital or established in the first three years of life. The attraction to children may surface already in the late pre-teens or early teens. Although there are unrecorded figures, estimates suggest that 1–2% of the population are paedophiles. It is possible to be a paedophile with a heterosexual or homosexual orientation, i.e. to be attracted to children of a particular sex. All paedophiles are not criminals. Not all paedophiles commit abuse, and not all sexual offenders are paedophiles.

103 Paraphilia is a term used to refer to intense and persisting impulses that are egodystonic in nature (thoughts, feelings or actions that are perceived as alien, unwanted or contrary to a person's values and self-perception) and/or that, directly or indirectly, cause harm to others when the person acts on the impulses. Source: Presentation to police staff by Specialist in clinical psychology Svein K. G. Øverland. Øverland, S. K. G. (13.11.2024). *Fortid, framtid, trender, tanker.* Stine Sofies Stiftelse, Grimstad.

104 Norwegian Centre for Studies on Violence and Traumatic Stress (2023). *Digitale seksuelle overgrep mot barn og unge* (Report 3/2023). p. 47.

A sub-category under the umbrella of sexually motivated actors get sexually aroused from humiliating and inflicting physical pain on their victims. This pattern of arousal is known as coercive sexual sadism disorder (CSSD)[105]. Who the victim is – whether a child or an adult – is not necessarily of importance to the actor. But as children are more vulnerable to exploitation than most adults, they make easy targets. Although this is a much smaller group than other sexually motivated actors, it is just as relevant and, like other actors, constitutes a threat to children. Other serious conditions associated with this group of actors include substance addiction, personality disorders and psychopathy.[106, 107]

The common denominator of all of the actors mentioned above, is that the motivation is to do with *sexual arousal*. However, in the case of minors subjecting other children to abuse, a number of other factors also come into play. The US National Center on the Sexual Behaviour of Youth (NCSBY) points to four fundamental factors[108] in the development of problematic sexual behaviour (PSB)[109]:

1. Youth vulnerabilities and risks
2. Family adversity
3. Modelling of coercion
4. Modelling of sexuality

105 *Coercive sexual sadism disorder (CSSD)* is a new diagnosis of the ICD-11 coding tool, not to be confused with consensual sexual sadism between consenting adults (more frequently referred to as SM or BDSM). The new ICD-11 classification has not yet been implemented in Norway, but according to the Norwegian Directorate of Health, it is due to replace the ICD-10 classification by the end of 2029.

106 Norwegian Centre for Studies on Violence and Traumatic Stress (2023). *Digitale seksuelle overgrep mot barn og unge* (Report 3/2023). p. 54–55.

107 Lunde, A. L. (2017). Å nyte andres smerte. *Tidsskrift for Norsk psykologforening,* (7), pp. 619–621. https://www.psykologtidsskriftet.no/artikkel/2017as07ae-A-nyte-andres-smerte

108 The four factors are: 1) *Youth vulnerabilities and risks*, 2) *Family adversity*, 3) *Modelling of coercion,* 4) *Modelling of sexuality*. Source: National Center on the Sexual Behavior of Youth. (2025). *Understanding and Serving Adolescents with Problematic Sexual Behavior:* Engaging Youth, Caregivers and Communities. Dallas.

109 Refer to the text box on the next page.

In a Norwegian context, harmful sexual behaviour (HSB) is often used as an umbrella term encompassing both problematic sexual behaviour (PSB) and harmful sexual behaviour.

Whereas harmful sexual behaviour involves offensive conduct, threats, coercion or a significant imbalance of power, problematic behaviours can be inappropriate in relation to the child's developmental stage or cause emotional distress, but without the same degree of serious violation or harm.

The regional Norwegian violence, traumatic stress and suicide prevention resource centres point to some of the same factors in their description of the causes behind such behaviours: This may include (1) inherent characteristics of the child resulting in impulsive behaviour (e.g. ADHD) and unfortunate sexual experimentation. It may also include (2) emotional, physical or sexual abuse or neglect. Additional factors may be connected to the child's experiences and observations, for example of (3) one parent subjecting the other to violence and coercion, or (4) adults having sex in the child's presence.

Children and adolescents today have widespread access to technology and sexual content such as pornography, generally with no guidance from adults, with a potential to affect their sexual development. Research shows that such exposure may increase the risk of problematic sexual behaviour compared with youngsters who have not been exposed to such content.[110] This ties in well with the concerns raised by children and adolescents that pornography to little extent conveys important values such as consent and mutuality, and that it has led youngsters to take part in acts they perceived as transgressive, painful or offensive.[111] Media reports have documented a rise in popularity of some dangerous practices including sexual strangulation, a trend that has been linked to pornography. Together this points to a complex interplay between technological availability, exposure to sexual content and the – healthy or

110 Mori, C., Park, J., Racine, N., Ganshorn, H., Hartwick, C., & Madigan, S. (2023). Exposure to sexual content and problematic sexual behaviors in children and adolescents: A systematic review and meta-analysis. *Child Abuse & Neglect,* 143, Article 106255. https://doi.org/10.1016/j.chiabu.2023.106255

111 Save the Children Norway. (2021). *Et skada bilde av hvordan sex er: Ungdoms perspektiver på porno,* pp. 20–26. https://resourcecentre.savethechildren.net/pdf/rapport_et_skada_bilde_av_hvordan_sex_er_ungdoms_perspektiver_pay_porno.pdf

unhealthy – sexual development of young people. Juvenile sexual offenders consequently contribute to making the category "sexually motivated actors" even more complex.

Although a sexual interest in children can arise from exposure to child sexual abuse material, the causal link between exposure to CSAM and the actual commission of child sexual abuse remains uncertain. What we do know, is that the use of CSAM is the strongest available indicator of a sexual interest in children, whether congenital (paedophilia) or one that has developed over time (sexual interest / paraphilia). We also know that many of those convicted of child sexual abuse have also been involved with CSAM.

The main strategy of the police is to prevent crime. As a consequence, it is the police's job to protect children from falling victim to sexual abuse. In order to prevent sexual crimes against children, we need to understand what drives the offenders to commit the sexual abuse, both in terms of internal motivations and what may be ascribed to external influences. There is no easy, unequivocal answer to this, and there are a number of knowledge gaps. We do, however, know enough about the mechanisms in play to establish that this is not a problem that can be solved by the police alone. There is a need for more research, knowledge sharing, development of treatment courses and new rules and regulations that keep up with technological advances, as well as a revised "relationships and sex education" curriculum covering such aspects as healthy sexual development and sexual behaviours.

Partial assessments

Sexually motivated actors are a diverse group of people with complex and nuanced motivations and preferences. They make up a vast and intricate threat that is challenging to tackle. Offenders increasingly make use of digital enablers to approach and groom victims, carry out and document child sexual abuse whilst safeguarding anonymity, concealing their activity and streamlining the various stages of their crimes. Technology *highly likely* functions as an accelerator for sexually motivated actors, and the incidence of child sexual abuse will *highly likely* remain at its current level in the year to come.

Under 18's committing sexual crimes against other children add to the complexity of the actor gallery, and the potential root causes of sexually problematic and harmful behaviours are many and varied. It is, however *likely* that access to technology, massive exposure to sexual media content and lack of control mechanisms lead to an increase in under 18's committing sexual crimes against other children.

The global emergence of synthetic child sexual abuse material adds to the total volume of available stills and videos of child sexual abuse. There is *an even chance* that this increase in availability combined with the increased distance from the actual[112] child victims can cause more people to develop a sexual interest in children. Similarly, there is *an even chance* that exposure to CSAM can make actors with a sexual interest in children take the leap from watching child sexual abuse to committing abuse themselves, either contact abuse or online.

Uncategorised actors

This category encompasses all actors who do not fit in with any of the other profiles, or whose motivation has not yet been established. Some can act out of personal reasons such as excitement, curiosity or revenge. Others may commit criminal offences simply because they have the technical skills and want to prove something to themselves or others. This way they can, for example, increase their status in digital communities. This shows that not all cybercriminals follow a clear pattern. A clearer picture of this group may help reduce the risk of black swans – or unpredictable, unanticipated phenomena.

Cult members / The Com – extreme, violent online communities

In this report, the NCIS has chosen to refer to actors taking part in extreme, violent online communities as *cult members*. As mentioned on pages 29 and 47–48, this phenomenon was first recorded in Norway in 2022, and has seen an upwards trend in 2025, both at a national and international level. Based on current insight, the NCIS has included cult members under the profile heading "uncategorised actors". This is due to the often unclear and complex motivations of cult members. There are, nonetheless, some common denominators that help paint a picture of these actors.

Even though cult members have been radicalised and some of them have developed extremist ideas, they are not fundamentally driven by political or religious objectives, although some may have ties to far-right circles. On the contrary, they are driven by so-called *nihilistic* violent extremism based on a general hatred towards society and a desire to foment chaos

112 Foundation models that generate synthetic child sexual abuse material have been trained on material featuring real children, both children subjected to sexual abuse and other children. In this context the term *real* refers to genuine stills and videos of real-life children.

and social disruption. Just like other cults, the networks are often organised around charismatic leaders.

The NCIS is also aware that most cult members seek acceptance, belonging, popularity and recognition. The more extreme a cult member gets, and the more serious the acts they make their victims commit, the higher status they achieve in the eyes of the other cult members. Based on this, it appears that many cult members long to be seen and to be part of a community, and that social exclusion and marginalisation may be among the factors that either draw them to these online communities or make them easy targets for recruitment into the communities. It is uncertain whether the actors themselves understand or are conscious of their own motivations. There are examples of victims who have become perpetrators and go on to seek out new victims. In many cases, guidelines and instructions as to how cult members should make preparations, identify victims, deceive and manipulate them and, finally, pressure them into committing serious offences, are shared with the community. The preparations include a number of steps to improve operational security and make them harder for the police to identify. In the NCIS' experience, cult members tend to opt for usernames without

The following behavioural changes could be an indication that a child or adolescent is influenced by a dangerous online community:

Online activity surrounded by secrecy: Hides the screen when someone approaches, uses multiple or anonymous accounts.

Withdrawal and isolation: Spends an unusual amounts of time on their own, distancing themselves from family and friends.

Emotional distress: Has sudden mood swings, appears anxious or depressed.

Interest in harmful content: Shows an interest in violence, dark topics, extremist ideologies or graphic content.

Changes in language or use of symbols: Uses unknown slang expressions, extreme language, codes or symbols that may be linked to extreme online communities.

Concealment of physical injuries: Wears clothes that covers self-harm, teeth marks, burns, cuts or other injuries or marks.

geographical clues and communicate in English. The networks are almost entirely international, and national sub-groups are rare.

The police receive information about persons with ties to extreme, violent online communities through ordinary tip-offs about CSAM, for example through NCMEC. Initially, it is often unclear whether the person mentioned in the tip-off is the offender or a victim who has been threatened or pressured into sharing CSAM of themselves.

The offenders are mainly boys and young men aged 12–25. This is also true for Norwegian actors. Several of the Norwegian cases included the planning or commission of extremely serious acts of violence or sexual crime.

This phenomenon gives rise to great concern as it can be both hard to detect and have extremely serious consequences. Children and adolescents can be pressured into performing acts spanning from self-harm via serious sexual acts on themselves or others to severe violence, murder and suicide. It is crucial that the police and society in general are aware of the existence of extreme, violent online communities and know what danger signals to watch out for.

Partial assessments

The unclear, and *likely* complex, motivations of cult members makes this threat hard to identify, uncover, investigate and prevent. Whilst many cult members are *likely* to be unaware of their motivations, it is also *likely* that a longing for recognition and a sense of belonging drives them to commit acts they would not otherwise have engaged in.

Cult members are concerned with operational security and communicate mainly in English, largely on encrypted messaging platforms. Networks are complex, with branches in all corners of the world and in constant expansion. The police are therefore *likely* to struggle to identify cult members who commit crimes against children and adolescents in Norway.

Some of the actors are *likely* to be easily led, and, consequently, vulnerable to manipulation and radicalisation. However, as some of the actors are also *likely* attracted to the transgressive aspect of the cults, there is *an even chance* that they might just as well have become involved in "pedo hunting" or been recruited by a criminal network to commit violence-as-a-service.

> Children and adolescents can be pressured into performing acts spanning from self-harm via serious sexual acts on themselves or others to severe violence, murder and suicide.

Photo: Shutterstock

Processes and methods in cybercrime

This section discusses the various *attack phases* and *target selection processes* involved in cybercrime. Figure 6 is a visualisation of roles and enablers, projected onto a circle representing cyber-dependent and cyber-enabled crime and, around it, other crimes taking place outside the digital space (cf. figure 1). The visualisation gives a clearer overview of how various types of crime relies on the digital space, and helps widen the analytical framework.

Attack phases and measures

The attack phase of a cyberattack should be understood as a process involving a number of intermediate objectives, decision points and actors. The degree of targeting, sophistication, motivation and intention may vary throughout the process, depending on the actor and the motive behind the act.

As shown in Figure 3 on page 56, (*The ontology of cybercrime*), criminal actors must generally complete a number of steps (intermediate objectives) to attain their final goal.[113] This is why cyber-dependent crime can be compared to a relay race – not a sprint – in which the baton changes hands several times before it crosses the finish line. The process comprises a number of decision points where the threat actor must make decisions based on the information gathered up to that point. These decisions have a bearing on how the remainder of the attack plays out.

The steps comprised in the attack phase vary depending on the type of crime, the approach chosen by the actors involved and the motive. Yet, through the course of their investigations, law enforcement agencies and security companies have uncovered some common denominators of the attack phases of for example ransomware attacks,[114] cyber-enabled fraud[115] and cyber-enabled sexual crime[116].

By mapping the decision points, intermediate objectives and involved actors in an attack phase, we can gain valuable insight into the dynamics of interaction between various activities and roles presented in Figure 4 (*the ARPA framework*) on page 60. This insight can help identify opportunities for disruption and targeted measures, and must be considered in light of the use of hybrid means and state actors'

113 Europol. (2025). *Internet Organised Crime Threat Assessment (IOCTA).* pp. 13–15.

114 E.g. illustrated by Europol through the Cyber Kill Chain® and MITRE ATT&CK®.

115 E.g. illustrated through the Fraud Kill Chain, Check Fraud Kill Chain and Financial Fraud Kill Chain.

116 E.g. shown in the diagram developed by the NCIS to explain some *Typical approaches used to establish contact with children* in *Cybercrime 2025*, p. 81.

Figure 6: Reliance on the digital space. The model shows that the same roles and enablers are found in both cyber-dependent and cyber-enabled crime. Their position in the model indicates to what extent the role or enabler is considered to be cyber-dependent (mid circle), cyber-enabled (outer circle) or outside the digital space (outside the circle). The latter category falls outside the definition of cybercrime, but has been included in the model to illustrate the short distance between cyberspace and the physical world. Where a role or enabler overlaps with more than one circle, this means that different aspects of the role or enabler can be found in different places on the cybercriminal spectrum. Hexagons are roles (facilitators and perpetrators), and ellipses are enablers. Facilitators have a dotted line and perpetrators a solid line. Orange elements are elements that are mainly found outside of the digital space. As for the elements found inside the digital space, roles are red, and enablers green. The enabler called "Malicious AI model" overlaps with the innermost circle ("Cyber-dependent perpetrators"). This is to illustrate that AI agents have the potential to function as independent perpetrators without human involvement. Model prepared by the NCIS.

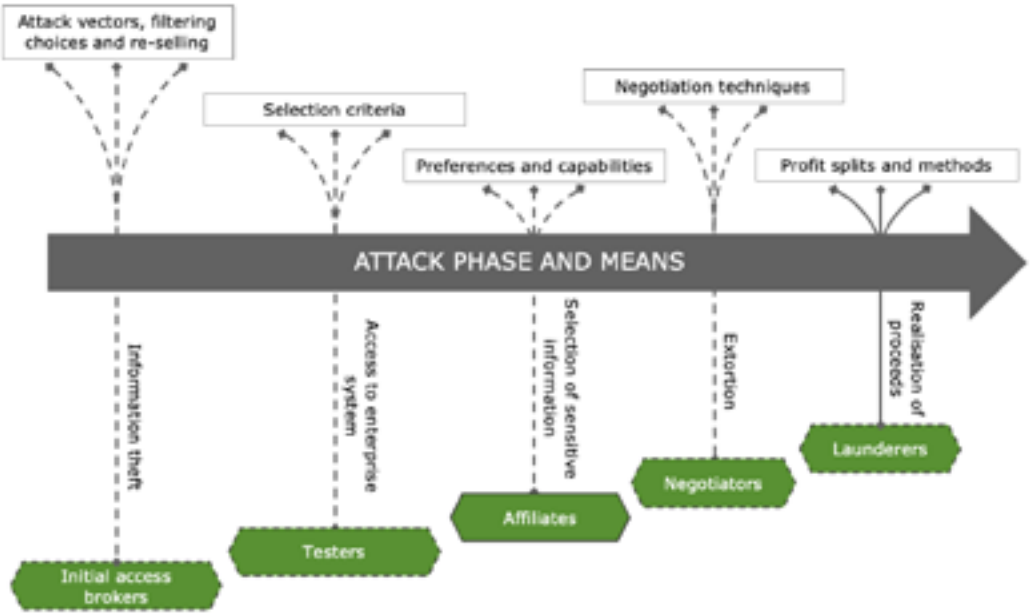


Figure 7: *Example of the attack phase of a cyberattack without encryption virus.* The model features five decision points (text boxes above the process arrow) and five intermediate objectives / final goals (below the process arrow). Dotted lines are intermediate objectives, whereas the solid line illustrates the final goal. Green elements at the bottom of the diagram link the objectives and decisions to the actors involved (hexagons with a dotted outline are enablers, and the hexagon with a solid outline represents the perpetrators). The process includes everything from the choice of attack vector (decision point) used by the initial access broker (involved actor) to steal information (intermediate objective), to how the proceeds are laundered and distributed (final goal) between the involved actors. At each decision point, various preferences and criteria influence how the attack plays out. Some decision points can therefore be extremely targeted, other more opportunistic. Similarly, some intermediate objectives / final goals can be achieved using high-tech cyber-dependent means, whereas others can be achieved using low-tech cyber-enabled means. Model prepared by the NCIS.

taking an interest in information offered for sale by criminals.

Figure 7 is an example of what an attack phase may look like.

Although a cyber-dependent attack process can start at a number of different decision points, it generally starts with a computer intrusion. From relatively simple operations with few intermediate objectives, cyber intrusions have developed into complex processes where a number of intermediate objectives (measures) must be completed to circumvent the user's security mechanisms. The increased level of difficulty has contributed to greater specialisation and distribution of tasks amongst criminal actors, resulting in new roles and activities in the cybercriminal ecosystem. Conversely, it is also possible for a single individual to take on all roles and carry out the entire attack process alone. This kind of comprehensive approach, in which a single actor completes all intermediate objectives from start to end, is unusual in cyber-dependent crime but more common in cyber-enabled crime, including some types of sexual offences.

The NCIS is aware that some data brokers[117] use the same means and approaches, but sell the information or access on to various buyers. A data broker can for example (1) offer large, unsorted datasets of a basic quality for sale on criminal market places; (2) sell access to organisations that constitute attractive targets for ransomware actors; or (3) sell data likely to be of interest to state actors through open or closed channels. Each of these examples involve different relationships, collaboration mechanisms, communication platforms and actors.

Selecting and approaching targets – cyber-enabled sexual crime

Cyber-enabled sexual crime against children encompasses a broad range of crimes that either target children *directly*, for example when a perpetrator sends texts of a sexual nature to a child on a social media platform, or *indirectly*, for example when two actors exchange CSAM obtained online. This sub-section will focus on sexual offenders targeting children directly with cyber-enabled sexual crime, regardless of the actors' profile or basic motivation.

In the case of sexual offences committed against children, all intermediate objectives toward the final goal are usually completed by a single perpetrator. The entire process, from contact is established to the sexual offence has been committed, tends to be carried out by the same actor. Furthermore, although there have been examples of actors targeting a specific child, it is the NCIS's experience that actors

117 Data brokers are people buying and selling data.

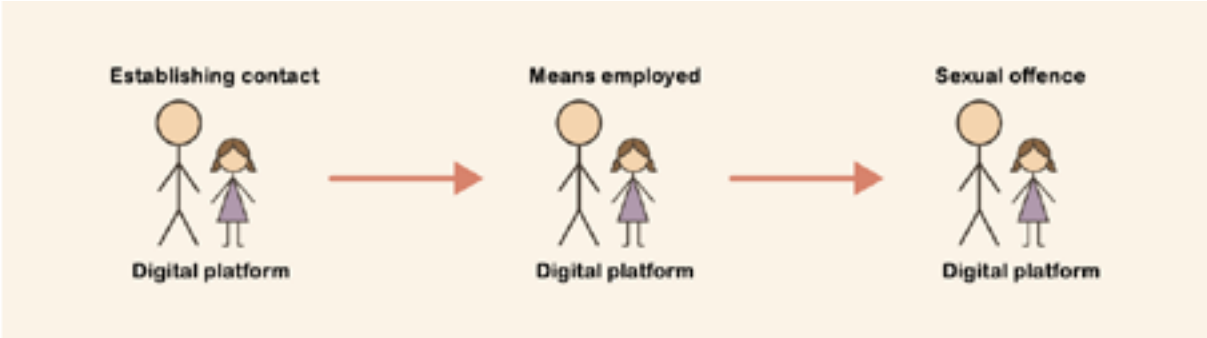


Figure 8: *Simplified illustration of the approach used by actors seeking to groom children for the purpose of committing child sexual abuse.* The illustration should be interpreted in light of figure 13, p. 81 of the *Cybercrime 2025* report. Model prepared by the NCIS.

in most cases approach random children. The perpetrators often cast their net wide, for instance by adding a high number of users on Snapchat or logging into a chatroulette platform and moving from one video chat to another in search of potential victims.

But many sexual offenders are also preference driven[118] and search for specific preferred characteristics. For example, some sexually motivated actors seek out arenas popular with a specific age group. Actors attracted to prepubescent boys may for example interact with the users on a Discord server for a video game popular with boys in the preferred age group.

Amongst the more determined actors are members of cult communities who actively seek out vulnerable children and adolescents. According to a Europol report on extreme, violent online communities, [119] these victims are easier to manipulate, and more trusting than other people. Children and adolescents between the ages of 8 and 17 who for example struggle with depression or suicidal thoughts, are part of the LHBTQ+ community, or come from a minority background are particularly vulnerable. Members of cult communities have been known to use forums such as online support groups and self-help communities to look for new victims. They build trust, gather personal information about the child, and move

118 The term "preference" refers to what an individual prefers when faced with multiple options.
119 Europol. (2025). *The rise of online cult communities dedicated to extremely violent child abuse.*

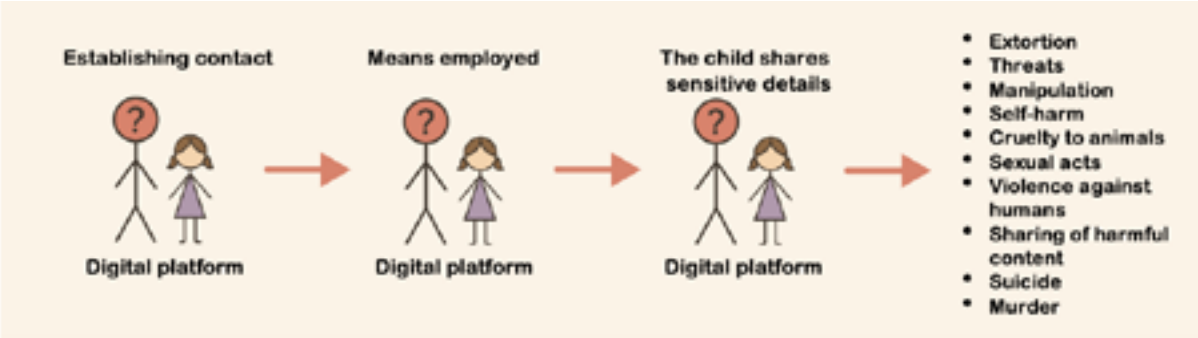


Figure 9: *Simplified illustration of the approach used by cult members to approach vulnerable children and adolescents, and the acts these victims are subjected to or coerced into committing.* The list of outcomes on the right is not exhaustive. The model is based on figure 12, p. 76 of the *Cybercrime 2025* report showing examples of the various stages of sexually and financially motivated sexual extortion. Model prepared by the NCIS.

the communication to an encrypted communication platform. The personal information obtained is then used to coerce and threaten the child into performing serious acts such as severe self-harm or sexual acts on themselves or other persons. The child is pressured into documenting the acts and sharing the material with the cult member, often as part of a series of other serious acts. Some actors also recruit new members to the online community. These often start out as victims, but with time, they are pressured or deceived into recruiting new victims.

Some of the actors have an opportunistic approach to crime and commit abuse when the opportunity arises, but apparently with no original intention to do so. One example is people who initially come online to see live streaming of pornographic content involving adult women, but who are offered to buy LDCA of underage girls. Another example of opportunism are profit-motivated blackmailers who mainly target financially able adult men. If the blackmailer gets into contact with a boy under 18, they will still deceive the boy into sharing a nude photo of himself before extorting money from him.

Technology enlarges the scope of action of actors committing cyber-enabled sexual crime against children. As mentioned in previous issues of this report, actors make use of digital enablers to conceal their identity, deceive children and reach out to higher numbers of children in more arenas, faster. In addition, the lack of control mechanisms gives the actor the scope to commit the abuse. Translated into a cyber-dependent context, this would be the equivalent of having either no firewall at all or an unconfigured firewall where some ports

have been left open. The lack of control mechanisms applies to both *safety and security*. This can include everything from the ability of a platform to protect children against crime on the platform (security), to the parents' involvement in their children's lives and their use of the available parental control features of the platform in question (safety).

Selection of targets – cyber-dependent crime

This section builds on the example in Figure 7. As a first step in the attack phase, the initial access broker (IAB) may obtain login details or access through for example phishing[120] campaigns targeting large email databases or the use of malicious web pages with a high ranking in search engines.[121] A wide net is cast to catch an as high number of internet users as possible. The IAB can for example sell login details (usernames and passwords) or provide access by installing malware[122] connecting the users' computers to a botnet[123].

In both cases, an initial access broker can assess the value of the material based on a number of selection criteria. The login details can, for example, be sorted by top domain, name and password strength. Access via compromised computers is considered based on more technical criteria such as cookies, IP address, operating system, computer name, digital wallets and whether or not the computer has an antivirus system. Using certain selection criteria, the compromised systems can then be divided into categories such as (1) high-value targets, (2) ordinary users; and (3) systems of no interest. The IAB can then offer to download ransomware to "high-value targets", install stealers on the systems of ordinary users and dismiss systems deemed to be of no interest.

It is only natural that IABs, who tend to cast their nets wide, apply quantitative selection criteria to process large data volumes. If

120 For example by sending out emails enticing users to click on a malicious link or download an attachment.

121 This is known as SEO poisoning.

122 Usually a dropper. A dropper is a computer application designed to install ("drop") other malware such as loaders and stealers onto a computer system. Malware increasingly uses a combination of different features. The dropper does not usually include malicious code as the computer application is designed to circumvent security mechanisms such as anti-virus systems on the victim's computer.

123 A botnet is a network of compromised computers and other online devices that have been infected with malware and, consequently, can be controlled remotely.

Photo: Shutterstock

login details or access are sold on to an EaaS grouping, qualitative selection criteria will often govern the next step. The criteria used by EaaS groupings can be business-related[124] or related to specific vulnerabilities[125], security issues[126], political issues[127] or reasons *not* to harm a specific organisation[128]. The criteria can change fast, and the limitations that apply to the affiliates using a specific RaaS may be different to those of its core group. If access was obtained through a third-party attack[129] or supply-chain attack[130], this will greatly impact the target selection process. Taken together, this emphasises the challenges associated with threat assessments based solely on the type of malware.

The NCIS does not hold any information to indicate that ransomware attacks may be directed at Norwegian organisations or businesses *because* they are Norwegian. This does not rule out that Norwegian organisations may be targeted, but the NCIS does know of any

124 E.g. turnover, domiciliation, number of employees and industry and the likelihood that the organisation will seek to avoid public exposure and reputational damage.

125 E.g. sector-specific or industry-specific vulnerabilities or vulnerabilities in shared technological infrastructure.

126 E.g. the likelihood of the organisation reporting the matter to the police, and whether the police will give priority to the matter and allocate resources to an investigation.

127 E.g. increased demand for access to Israeli and American organisations in the wake of the war in Gaza.

128 Some RaaS groupings have explicit guidelines on whom not to target, e.g. NGOs working with children, the health sector, the energy sector, schools and the military sector. The reasoning behind this may be fear of prosecution or internal ethical standards.

129 Third-party attacks is the exploitation by criminal actors of a vulnerability at a third party to access one or more other organisations. A third-party attack can be combined with a supply-chain attack, but the two methods are in no way interdependent. Simply put, whereas a supply-chain attack targets a specific technology, a third-party attack targets the entire vulnerability surface of an organisation.

130 Supply-chain attacks happen in the product development process, before the product or product update is deployed, and is typically carried out by an unauthorised actor adding or modifying either existing code or physical components of the product. These modifications can be exploited at a later stage.

cases where Norwegian nationality as such has featured among the selection criteria of profit-motivated EaaS networks. The opposite is true for hacktivists, who sometimes also make use of encryption viruses and commit data theft.

It is hard to determine what has actually happened in a cyberattack and what harm has been inflicted on the victim organisation without investigating the offence. In an investigation, the main focus of the police is to identify the perpetrator – not to reconstruct the ideas that laid the foundations for the target selection. As part of the initial enquiries, the police follow the leads back to their origin. If the police note that, for example, login details or system access have been obtained using a *wide net*, the attack may be interpreted as opportunistic. However, as illustrated by the attack phase decision points (figure 7), following a lead back to its origin can only reveal where the data originated from. It does not provide any insight into the train of thought of the perpetrator or the choices they made in the process.
The description of the attack phase is included here to provide insight into the process, from the selection of a suitable attack vector to the exploitation and realisation of the target, which often involves a number of actors, decision points, preferences and trade-offs. Cyberattacks that appear to spring from a wide, opportunistic access may have involved some very deliberate choices at other stages of the attack process. Investigations, by their very nature, tend to be backward-looking. However, if we are to properly understand the attack phase and the level of determination of the threat actor, the decisions that shaped the way towards the final goal should be considered in a forward-looking perspective.

Criminal networks' use of digital enablers

As previously mentioned, technological advances have provided criminal networks with the opportunity to expand their operations, both nationally and internationally. The internet functions as a market place for everything from drugs to criminal services. Through social media and encrypted platforms, the networks can reach out to a much bigger audience, recruit new members and sell goods and services anonymously, without in-person contact. Technology has made it easy for foreign actors to establish themselves in Norway where, particularly, Swedish networks have upped their presence recently.

Criminal networks increasingly use technical platforms to recruit people to carry out various tasks such as transport, storage, drug dealing and money laundering. Recruitment can be covert or overt, and the police have uncovered attempts to recruit people whose profession gives access to information, goods or services susceptible to be exploited.

Criminal networks traditionally have a strong hierarchical structure with clear leadership and

responsibilities. For some criminal networks, particularly those with a high level of digitalisation, the emergence of CaaS in the digital space has fragmented this structure and made it more flexible. Actors increasingly collaborate across networks and national borders, and profit tends to speak louder than loyalty.

This evolution is similar to that of the cybercriminal ecosystem, with specialisation, buying and selling of services and skills-based collaboration at its core. Yet, whilst cybercriminal networks are entirely digital, criminal networks operate in a hybrid space bridging the physical and digital spheres.

The greatest dissimilarity is that whereas cybercriminals can operate on a global scale without ever leaving their computer, traditional criminal networks rely on a local presence and physical implementation in the areas where they operate. Technology, therefore, primarily works as an amplifier for existing crime rather than a replacement for physical capacities. Technology is a digital enabler helping to streamline logistics, recruit persons into local roles, communicate securely and reduce the risk of detection of organisers.

Partial assessments

It is *highly likely* that criminal networks will continue to integrate technological tools to streamline operations and maximise profits. As criminal networks increasingly rely on digital enablers to optimise operations, there is *an even chance* that the lines between traditional criminal networks and cybercriminal networks will become blurred in the long run.

The emergence of violence as a service

The evolution of CaaS has provided criminal networks with the opportunity to tweak the concept into what has become known as violence-as-a-service or VaaS[131]. Through digital platforms, criminal networks reach out to a wide audience – particularly vulnerable youngsters – who are lured, deceived, motivated or coerced into committing violence on behalf of the criminal network.

Swedish criminal networks recently established in Norway use social media actively to attract vulnerable young people. Through rap music and a deliberate use of symbols and imagery glorifying gang culture and violence they normalise the criminal life-style and project an image of themselves as tough and intimidating.

131 NCIS. (2025). *Vold som handelsvare – En beskrivelse av fenomenet.* https://www.politiet.no/globalassets/tall-og-fakta/kriminelle-nettverk/2025-10-16-a-vold-som-handelsvar---kripos_.pdf

> Technology is used as a digital enabler to streamline logistics, recruit persons into local roles, communicate securely and reduce the risk of detection for the organisers.

Photo: NCIS, AI-generated

Motivations of young persons recruited into criminal gangs:

Initial stage: Through promises of fast cash, excitement and the perceived high status associated with the gang's brand, vulnerable adolescents are lured into contacting the gang. Recruiters promote an image of luxury, power and a sense of belonging that the youngsters can take part in.

Intermediate stage: Throughout the luring process, the sense of community and loyalty becomes more important than the money. Recruiters build a relationship of dependence and make the youngster feel unique and important to the network. The lure of financial gain is strongly downplayed in this phase, and the sense of having a role in the community dominates.

End result: In reality, there are few examples of young people actually receiving the payment they were promised once their mission has been completed, and there is little to suggest that they actually achieve a higher status within the group. The youngsters lose out and are exploited as disposable resources.

Many vulnerable young people are inspired by the image projected by the gangs, and the criminal networks use social media for recruitment. Whilst the recruits are lured in through social media[132], the actual publication of VaaS ads, planning and coordination often takes place on encrypted communication platforms[133].

A distinct trend in the past year is that recruitment to VaaS has spread from encrypted platforms only, to include open platforms such as social media sites, thereby widening the recruitment pool. At the same time, there has been an increase in VaaS in Norway. In 2025 the police recorded double figures of VaaS assignments carried out in Norway, and averted just as many. This illustrates the important role of technology in the criminal networks' operations.

Vulnerable youngsters recruited through social media

Those who accept VaaS assignments for criminal networks, and who appear to be the intended target group for these job postings, are often vulnerable young persons. Recruiters sometimes argue that they need not worry about penal sanctions as they are below the age of criminal responsibility.

132 TikTok, Snapchat and Instagram are the most widely used.
133 E.g. Signal, Telegram and Zangi.

The recruitment process can move extremely fast. Sometimes it is only a matter of days from the initial contact to the youngster is holding a gun in their hand. In other cases, perpetrators are recruited without there being a specific attack in the pipeline. In the latter case, it can take a while before the perpetrator is activated, but this is primarily due to lack of jobs and not down to a lack of willingness or motivation on the part of the perpetrator.
Meanwhile, the perpetrator is kept "warm" through digital communication where the perpetrator is told how important he is and that the network needs loyal and fearless "soldiers". This helps maintain motivation until a target has been identified.

Technology has enabled this kind of CaaS, where organisers operate from transit countries without an extradition treaty with Norway, controlling the crime remotely down to the smallest detail. Technology is key in all parts of the process, from recruitment and planning to the commission of VaaS.
Once the attack has been completed, news articles, videos of the incident or other references to the attack are used as propaganda on social media to establish an intimidation capital, control the reputation of the network and recruit new perpetrators. Without the availability of technological tools, neither the rapid establishment of criminal networks in Norway nor the controlling of violent attacks from remote locations would have been possible.

Partial assessments
It is *likely* that the sense of belonging and social status within the criminal network is just as important to young perpetrators as financial gain.

In 2025, a record number of known VaaS assignments were ordered through social media and encrypted communication platforms. It is *highly likely* that there will be new VaaS incidents in Norway in 2026.

If Nordic authorities succeed in arresting organisers, for example through international cooperation, arrests in other countries and the application of extradition treaties, this will *likely* reduce the prevalence of VaaS in Norway.

Photo: Shutterstock

Expected developments in 2026

In the *Cybercrime 2024* and *2025* reports, we split our threat assessment into three categories, namely *threats against individuals, against organisations* and *against society as a whole*. However, these three categories are becoming increasingly intertwined. A threat against individuals can spread to business networks, and the consequences of an attack against an organisation may spill over to society as a whole. Vulnerabilities and dependencies are therefore independent of such categories. A compromised mobile phone may constitute a gateway from an individual to society. Additionally, threats directed at many individuals may impact the wider society.

The threat against individuals

The evolution of the human-machine interface (HMI) is *likely* to continue, also in the field of CaaS, resulting in a lowered threshold for use and increasingly complex, high-performance tools. Increased professionalisation and specialisation within the field of CaaS is *likely* to drive this development. Moreover, it is *likely* that such a development will lower the barriers to entry for new criminals, and that children and adolescents will be targeted for recruitment to carry out simple, but often relatively high-risk, assignments on behalf of others.

Profit is a strong motive for many actors in the cybercriminal ecosystem, and criminals constantly tweak their methods and approaches. As some sexual offenders are motivated by profit, there is *an even chance* that the increase in and evolution of crime-as-a-service, including VaaS, may also spread to the field of sexual crime.

Furthermore, it is *likely* that the knowledge gap between private individuals and organisations that exists in the area of digital threats and security, will widen as criminals continue to adapt to counter-measures and develop new and more sophisticated methods. Threats from the digital domain are increasingly complex,

and this trend is compounded by the so-called "black box" of AI[134]. Very few private individuals have the interest, time, energy or skills to safeguard their own security. At the same time, the private and professional spheres become increasingly intertwined, and many work-related tasks are carried out on personal mobile phones and computers.

Private individuals who want to safeguard their own security, must purchase security solutions from trustworthy professional providers. Those who do not, will become extremely vulnerable to digital threats. It is *likely* that the knowledge gap is at its widest in the youngest and oldest age groups, as well as in some vulnerable groups. It is also *likely* that unprotected private individuals will become more attractive as targets of cyber-dependent crime and information gathering.

The combination of technology and a lack of maturity makes it *likely* that children and adolescents will become more vulnerable to sexual exploitation. Sexually motivated actors increasingly make use of digital enablers to approach and groom their victims, carry out and document child sexual abuse, safeguard their anonymity, conceal their activities and streamline the various steps of the offences. It is *highly likely* that technology functions as an accelerator for sexually motivated actors, and it is *highly likely* that the incidence of child sexual abuse will remain at its current level in 2026.

It is *highly likely* that 2026 will see an increase in cases linked to extreme, violent online communities and that Norwegian children and adolescents will be amongst the perpetrators as well as the victims. It is *likely* that more Norwegian perpetrators and victims will carry out serious acts as a result of their involvement in these online communities, thereby placing themselves and others in grave danger.

The threat against organisations

Destructive cyberattacks are generally more difficult to carry out than disruptive attacks, as the physical or logical destruction typically demands in-depth knowledge and a thorough understanding of how the system works. For this reason, it is *likely* that a possible destructive cyberattack targeting Norwegian organisations or critical infrastructure will be carried out by an actor in possession of inside information or trusted access to systems.

Destructive cyberattacks are *unlikely* to be carried out by profit-motivated criminals in the coming year. On the other hand, Norwegian organisations that directly or indirectly support critical infrastructure and public functions are *likely* to be targeted by EaaS networks.

It is *unlikely* that hacktivists alone, without the support of a state actor, will be able to car-

134 "The black box of AI" is an expression used to describe the opacity of an AI system. The user cannot possibly know what happens inside the system, hence the expression "black box".

ry out destructive cyberattacks against critical infrastructure in Norway.

There is *an even chance* that the increased use of modern security mechanisms[135] and improved basic security hygiene will lead to more widespread use of social engineering techniques and exploitation of inherent features[136] of the victim's systems and less use of malware.

If legal international digital supply chains are disrupted, there is *an even chance* that cybercriminals will seize the opportunity to create apparently legitimate organisations to fill the vacuum, as a high pressure to fill gaps in the supply chain will *likely* lead to less critical scrutiny of new actors. Should this happen, there is *an even chance* that the actors will also gain increased access to Norwegian organisations. In such a case, and in the event that Norwegian organisations are targeted by attacks, this will *likely* take the form of third-party attacks.

It is *likely* that new EaaS groupings consisting of young cybercriminals will implement new methods, particularly relating to social engineering, public communication and marketing and the use of artificial intelligence, to commit their crimes. Young cyber-dependent criminals are *likely* to be less predictable in their choice of targets and not stick to the same, typical approaches favoured by the more established ransomware groupings in the past five years.

The implementation and use of AI agents by organisations is *highly likely* to be exploited by criminals. Moreover, it is *likely* that AI agents used by Norwegian organisations will help cyber-dependent criminals working from the inside of the organisation's network to quickly identify sensitive information and pressure points that can be exploited by the criminals in a blackmail situation.

The threat against society

Hacktivism is an increasing threat against persons with prominent positions in society, who, for example, represent certain political views or values. There have been several examples of personal attacks against elected representatives. Technological advances facilitate targeted, more sophisticated and scalable attacks, and there is *an even chance* that such attacks will raise the bar for taking part in public debate.

Attacks carried out against democratic symbols and processes by politically or ideologically motivated actors who, by barring access to information, misusing political symbols or brands or changing existing content, seek to put a message across and weaken trust, show that hacktivists target the credibility and legitimacy of democratic institutions. Such manipulations of symbols and disinformation campaigns are *likely* to evolve in both sophistication and scale

135 E.g. *Endpoint Detection and Response (EDR).*
136 *Living Off The Land (LOTL).*

in 2026 onwards, particularly in connection with elections and political conflicts.

According to a previous assessment by the NCIS, AI-generated content is *highly likely* to challenge the general level of trust in society. This does not only concern trust in digital content shared by individuals, mass media and institutions but also digital communication between people. This assessment still applies for 2026 and the coming years.

It is *likely* that AI-generated program code will lead to a relative increase in the number of software vulnerabilities, and that this will continue to be true for a while after AI models have surpassed humans in uncovering vulnerabilities in program code. It is further *likely* that AI-generated code containing vulnerabilities will spread to open-source code software, and that this will be exploited by criminals.

Actors who commit sexual offences, regardless of their motivation, constitute a threat to the most vulnerable in society – our children. Ultimately, these actors also pose a threat to society given the prevalence of their crimes and the consequences suffered by the affected children. It is *likely* that the total threat from sexual offenders will increase in 2026, in particular given the rising number of The Com-related cases in Norway and the ability and willingness of profit-motivated actors to find new ways of making money. Moreover, it is *likely* that increased access to and scale of technological enablers, combined with the lack of effective control mechanisms, increase the risk of children falling victim to sexual abuse or of developing problematic or harmful sexual behaviours or other deviant behaviours, which may, in turn, cause them to become perpetrators themselves.

It is *likely* that AI contributes to depressing prices of many digital goods and services available on criminal market places, such as *phishing kits*[137] and digital tools used to commit crime.

There is *an even chance* that some refugees and migrants arriving in Norway from Ukraine possess technological skills that are valuable to Norwegian criminal networks. Furthermore it is *likely* that Norwegian criminal networks will actively seek to recruit cyber-dependent criminal actors to increase their capabilities in areas such as scouting, surveillance and operational security.

It is *highly likely* that crime-as-a-service (CaaS) will require more resource-consuming investigations due to increased distances between organisers and perpetrators, use of anonymity technology and declining knowledge of local actors due to an increasing number of involved parties and the inherent characteristics of the digital sphere.

137 A phishing kit is a ready-made package containing various software tools that enable cybercriminals, regardless of their level of technical skills, to carry out a phishing campaign.

Photo: Shutterstock

Annex

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

Probability levels

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

Glossary of terms

The fast innovation rate within the field of digital technology is to a large extent due to widespread international cooperation. Technological innovation gives rise to new terms to designate new concepts. The new terms are generally coined in English first.

In Norway, it is the NCIS's responsibility to define and develop a specialist terminology for cybercrime. This includes defining a number of concepts that are specific to the fields of technology, crime, safety, security and functions of society, but which may have other meanings in other contexts. Based on the above, we have opted to include an updated glossary of terms in each new report.

Criminology

Cybercrime covers a wide array of offences ranging from cyber-dependent to cyber-enabled crime and comprises all kinds of crime committed by means of or facilitated by information and communication technology, including computer systems, networks, devices and software. Refer to the *conceptual map* (Figure 1) for a more detailed definition.

Type of crime refers to the crime set out in the relevant penal provision of the Norwegian Penal Code, but may also denote phenomena, e.g. sexual extortion, that do not have a section dedicated to them in the Penal Code. As there

are no established definitions of the terms "field of crime", "area of crime" and "type of crime" within the Norwegian police, uses may vary.

Cybercriminal ecosystem is an umbrella term for all criminal actors, comprising: (1) the actors committing the crimes, i.e. the criminal landscape, (2) the environment in which the crimes are committed, i.e. the digital space, and (3) external factors with a bearing on the criminal actors, e.g. political, psychological, technical, legal or financial factors. As a natural consequence of this ecosystem, the actors communicate, share, sell, interact, operate, compete and clash with each other. However, the cybercriminal ecosystem cannot be considered in isolation, and a number of its actors make a living by exploiting victims ranging from individuals to private and public-sector organisations.

Grey areas can occur at the intersection of different fields and categories. Limits between categories can be unclear for a number of reasons, and the resulting overlap is often referred to as a grey area. Grey areas can occur anywhere. In this report, the term "grey area" is used to refer to grey areas between various actors (profiles), when similarities in tools, methods and activities make it hard to distinguish between the actors.

Approach is used to refer to a particular course of action that cybercriminals tend to follow to achieve their goals, i.e. the methods used and the sequences in which they are applied to commit criminal acts. **Operational pattern** and **modus operandi** are related terms used in other contexts. An approach comprises a set of **actions** linked together in a concrete and volitional process with several stages of **activities**. Computer intrusions and the befriending of children are examples of actions. The capture, transfer, storage, adding, generation, modification, concealing and deletion of data are activities carried out in the digital space.

Incident is in this report taken to mean an event that can impact the safety and security of an individual or organisation, or of society as a whole. An incident arises from the voluntary actions of a criminal actor and involves at least two parties, an actor and a victim or a computer system. It can involve both cyber-dependent and cyber-enabled crime. The term "incident" can also refer to activities carried out to support criminal objectives and may occur in different parts of the chain of attack. An incident can occur whether or not an unauthorised third party has succeeded in their influencing attempts. Examples of incidents include scanning for open ports on a network, vulnerability mapping in software and attempts to recruit insiders.

Intervention, or **police intervention,** is a term used in this report to refer to the arrests, searches and other situations in which the police have actively intervened to stop criminal activity.

Technology

The term **technology** comprises knowledge, methods and tools used by humans to solve problems and meet needs. In this report, the term denotes modern technology (mobile phones, computers, AI) and invisible technology (software, internet, algorithms).

Cyber is a term that refers to all technology that, in addition to the physical infrastructure used to process, store or transmit information through electronic signals, relies on digital data. Such technology includes, but is not limited to, computers, radio equipment and the internet. **Cyberspace** is used in contrast to the physical sphere.

Digital space refers to a global domain of interconnected computer systems and information resources, and is used as a metaphor, in contrast to the physical space. In reports published by the NCIS, digital space refers to the totality of computer systems, networks, devices and software where cybercrime is committed.

System refers to an assembly of components connected together in an organised way to solve a problem. In this report the term "system" is taken to mean either a technological or a social system. **Technological system** is a man-made assembly of interrelated components organised in a logical manner that function together in a digital communicating ecosystem. A technological system comprises various components, relationships and links between components. Examples include computer systems, OT systems and enterprise systems. **Social system** is a term used to describe relatively long-standing relationships between individuals, groups or institutions, or between different social systems, in which the group members are in a defined mutual relationship to each other. A social system comprises processes that contribute to sustain, regulate, change or renew the systems, e.g. language, values, norms or laws. Examples include the cybercriminal ecosystem and cybercriminal networks or groups.

Operational technology (OT) refers to systems, devices and communications infrastructure supporting the production, supply and maintenance of physical goods and services, often in industry facilities or other large process environments. OT also includes hardware and software used to control other systems or devices that monitor or alter physical processes. See also industrial control systems (ICS). OT refers to an area of technology (in analogy to IT), whilst the term **OT systems** refers to a collection of physical and digital components (and

underlying systems) that are closely integrated to achieve an overarching goal.[138] The term is used in opposition to "enterprise systems".

Industrial control systems (ICS) is a sub-category of OT systems which includes various types of equipment, networks and systems used to operate and automate industrial processes. It can include components such as field equipment control systems and applications.

Enterprise system is a software solution designed to support a number of management and business-related tasks across an organisation. Enterprise systems can e.g. include modules for processing employee data, finance and administrative tasks in relation to production, sales and purchasing. IT systems are an integrated part of both enterprise systems and OT systems. However, in enterprise systems, IT systems are not directly involved in operational tasks. In this report, the term "enterprise systems" is used in opposition to "OT systems". Examples include enterprise resource planning (ERP), customer management (CRM) and business intelligence (BI) systems.

AI system is an umbrella term for various software and hardware solutions that perform physical or digital actions based on the interpretation and processing of structured and unstructured data, with a view to achieving a given objective.[139] **Foundation model** is an AI system that, in addition to having generative abilities, can be adapted to a range of different tasks, e.g. language translation, photo and audio analysis. Foundation models form the basis of a number of **AI applications**, including large language models, of which some of the best-known examples include Open AI: ChatGPT; Google: Gemini; and Anthropic: Claude.

AI agents can be described as automated robots that, independently or in collaboration with other AI agents or humans, carry out technological tasks either autonomously or guided by humans. This includes the use of digital tools and control of computer systems. Some typical characteristics of AI agents are interactivity, flexibility, reactivity and proactivity to find optimal solutions to problems. The most capable AI agents today consist of a layer of software design added to an existing foundation model. AI agents are sometimes referred to as "intelligent agents". Other AI systems may also

138 Saurabh, K. (2009). Systems engineering modeling and design. I A. Bajaj & S. Wrycza (Red.), *Systems Analysis and Design for Advanced Modeling Methods: Best Practices* (1 Ed., pp. 96–100). Imra International.

139 Ministry of Local Government and Modernisation. (2020). *Nasjonal strategi for kunstig intelligens*. p. 9. Government of Norway.

have **agentic capabilities** without necessarily being referred to as AI agents. Such capabilities can include objectives, actions, memory and rethink.

End-to-end encrypted messaging platform is a communications channel, e.g. Signal or WhatsApp, that uses end-to-end encryption. This means that only the participants in a one-to-one conversation or the members of a closed group messaging each other have access to the messages. Before messages and files are sent via the network they are encrypted with a key that is known only to the sender and the recipient. Audio and video messages can also be encrypted with end-to-end encryption.

The darknet is a small part of the internet consisting of networks using their own communication protocols. Navigating these networks requires specialised software.

Environment is a term used to refer to a geographically (and logically) limited area where a number of processes, units and systems interact to achieve a desired state or outcome. The term "environment" is used regardless of the technological domain. In an OT context, environment refers to the physical processes and digital support systems interacting to produce physical goods and services. Examples include OT environments, industrial environments, process environments, operational environments, business environments and IT environments.

Component is an umbrella term used to designate the individual parts of a technology. Components are the building blocks making up complex end-products such as instruments, hardware and software. Examples of components include switches, circuit boards and database modules.

Dual-use items refers to technology and services that, although intended for civil use, can also be used for military purposes. The term is here used in a wider meaning to include criminal applications.

Legacy systems are old, often outdated systems that are vulnerable to exploitation because they were developed at a time when the security situation was very different.

Botnet is a network of compromised computers and other online devices infected with malware, which can be remote-controlled without the consent of the users.

Black box of AI is a term used to refer to what is on the inside of an AI system. The term "black box" alludes to the fact that it is impossible for the user to know what happens inside the system.

Security updating is the process involving removal of vulnerabilities, bug fixing and strengthening of the system's defences against cyberattacks. **Patching** refers to the application of a software or system patch to remove a known vulnerability.

Values and assets

Supply chain and **value chain** are terms used

to refer to different aspects of certain stages of the production process.

Supply chain is a chain of businesses that are directly or indirectly involved in meeting a customer need. A supply chain spans a number of organisations and encompasses the flow of goods, information and money between them.

Value chain is a term used to describe how value is added to the products (goods and services) through the various links in the chain. The value chain can include multiple actors that either supply or demand inputs (goods and services) that go into the product. The term includes the full lifecycle of a finished product and encompasses the resources, processes and activities that go into the manufacturing of a product.

Third party refers to an external party in relation to the principal organisation in a business relationship, i.e. the party who initiates an assignment. A third party can be a service provider offering, e.g., banking services, cloud services or internet access. It may also be a sub-contractor, e.g. a manufacturer of hardware components or a supplier of raw materials, upstream in the supply chain. In some cases, clients may also be considered third parties due to mutual dependencies through, e.g., a shared data centre.

Victim refers to anyone who has been a victim of a crime or unwanted influence.

OT dependent and **IT centred** organisations are organised entities that supply services or carry out activities to achieve specific objectives. This includes public and private sector entities with objectives ranging from making a profit to supplying services to the benefit of society. Whilst OT dependent organisations rely on OT systems to be able to supply their goods and services, IT centred organisations are organisations that, despite having digital vulnerabilities, do not use operational technology to sustain their primary assets. Depending on the context, organisations are also referred to as risk owners, asset owners or facility owners.

Children, in this report, is taken to mean persons under the age of 18. The words boy or girl are used when a child's gender is known. For juvenile offenders, the report distinguishes between children under the age of 18 and under the age of 15, which is the age of criminal responsibility in Norway.[140]

Actors involved

Actor is a generic term used to refer to individuals and groups. It can e.g. be used to refer to a specific grouping that commits ransomware attacks. In such cases, the term "ransomware

140 Norwegian Penal Code. (2025). Ch. 1, section 20 subs. 1 a). *The Penal Code* (LOV-2025-06-20-86). Lovdata. https://lovdata.no/dokument/NL/lov/2005-05-20-28/KAPITTEL_1-3#KAPITTEL_1-3

actors" is used. **Threat actor** is a term used when it is neither possible nor useful to specify the actor's relationships and affiliations. The term can include state actors and terrorists as well as certain cybercriminal individuals and groupings. The term "threat actor" is also used when the actor presents a specific threat to an individual, organisation or computer system.

Criminal and **cybercriminal** are both used to designate individuals who commit crime. Whilst "criminal" is domain neutral, "cybercriminal" refers to a person who commits crime in the digital space. Crime aided by computer systems (refer to the conceptual map of cybercrime) is consequently committed by a category of criminals not referred to as cybercriminals in this report. **Offender** and **perpetrator** are alternative terms designating criminal actors and used for linguistic variation, particularly within the field of sexual offences.

Cybercriminal group is a term used to designate a collection of individuals who collaborate to achieve a common goal through the commission of cybercrime.

Criminal network is an umbrella term used to designate communities, gangs, groupings and sets of individuals who cooperate in their commission of crime. The criminal connections may be brief or long-lasting and involve all types of crime, and the networks can have a higher or lower degree of structure and organisation.[141]

Cybercriminal network is a term used to designate a collection of individuals and/or groups who collaborate, mutually depend on each other or exchange goods and services to commit cybercrime.

Core group is a term used to designate the innermost circle of cybercriminals in a RaaS system. The variant term RaaS grouping is also used to refer to the core group in some contexts.

Facilitator is a person who, through their access and competence, acts as an accessory to crime or helps conceal crime. **Perpetrator (offender)** is a person who commits crimes against individuals or organisations. The same actor can be a facilitator or a perpetrator depending on the situation.

Enabler is a term used to refer to technological tools, digital infrastructure and physical tools.

Affiliate is a person with a business-like relationship to a RaaS grouping and who uses ransomware-as-a-service.

141 Lunde, A. (24.08.2021). *Kriminelle nettverk innen økonomisk-, arbeidslivs-, og miljøkriminalitet.* Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime, p. 1. https://www.okokrim.no/kriminelle-nettverk-innen-oekonomisk-arbeidslivs-og-miljoe-kriminalitet.6353115-411472.html

Initial access broker (IAB) is a term used to designate cybercriminals who sell stolen information and unauthorised access to computer systems. The initial access broker is an example of a role often associated with the profile "profit-motivated criminal".

Insider is a term used to designate a person who exploits legitimate access to or information about the assets of an organisation for criminal purposes, on behalf of themselves or others. Under this definition, an employee who is deceived into clicking on a link or a file with harmful content, is not considered an insider.

Criminal proxies (proxy actors) are persons and organisations with no formal ties to intelligence or security services or other government agencies who, knowingly or not, carry out criminal activity on behalf or in support of state actors. The activity may be politically, ideologically or financially motivated.[142]

Capacities refer to the quantifiable features and assets of criminals. Examples include physical and mental stamina, the number of individuals in a group and digital assets. Together, a group's capacities and their ability to exploit them make up the group's capabilities.

Motive is what an actor wants to achieve through the criminal activity. Possible motives include financial gain, sexual gratification, social change, access to sensitive information and inflicting physical harm. The term "motive" refers to the fundamental driving force behind the actors' actions. **Motivation** is not only what an actor seeks to achieve (the objective), it is also the underlying reason why the actor wants to achieve a given objective.

Intention is a term used in this report to describe the overarching goal or ultimate purpose that actors put their efforts into achieving. More than just the sum of a number of specific plans and objectives, the intention describes the desired end state.

Criminal activities

Crime-as-a-service (CaaS) is a term used to refer to the sale and purchase of criminal services, software and tools. CaaS contributes to making crime profitable, financing new crime and making crime more accessible, including to actors who are unable to commit such crimes on their own.

Ransomware-as-a-service (RaaS) is a sub-category of CaaS, consisting of the sale or rental of existing ransomware. As an alternative approach, some actors develop and apply ransomware that is not sold or rented out to other actors, so-called proprietary ransomware.

Extortion-as-a-Service (EaaS) is a term encompassing traditional RaaS networks as well as criminal constellations who, whilst engaging

142 Norwegian Police Security Service. (2025). *Nasjonal Trusselvurdering 2025.* p. 12.

in other forms of cyber-dependent extortion, still operate within the framework of crime-as-a-service (CaaS).

Cyber-dependent extortion is an umbrella term encompassing various cyber-dependent MOs used by profit-motivated criminals to extort a ransom from victims. This can e.g. be, but is not limited to, ransomware attacks. Other examples are threats to publish sensitive information or repeated denial-of-service (DoS) attacks.

Digital vandalism is a term used in this report to refer to cyber-dependent criminal acts and activities that damage ICT systems. Examples are denial-of-service attacks carried out by hacktivists and acts of vandalism to critical infrastructure.

Cyberattack is an umbrella term used to designate various types of cyber-dependent crime, both actual and imagined scenarios, when it is not possible or practical to describe the unwanted acts in more detail. Examples of cyberattacks include computer intrusion and data theft, and destructive cyber operations with military implications, referred to as "digital vandalism" in this report. Cyberattack[143] is a punishable offence under the Norwegian Penal Code.

Chain attack is a form of attack that provides criminals wanting to target a large number of victims with the opportunity to exploit vulnerabilities in shared or connected hardware or software. There are several kinds of chain attacks, but in the context of this report, the term "chain attack" encompasses supply-chain attacks and third-party attacks. **Supply-chain attack** is a term used to designate an attack that happens in the product development process, i.e. before the product or product update is rolled out. The attack is typically carried out by an unauthorised actor by adding or modifying either existing code or a physical component of the product. These modifications can be exploited at a later stage. **Third-party attack** is a term used to describe the exploitation by criminal actors of a vulnerability at a third party

143 In Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, implemented as regulation in Norway, "cyber-attacks are [defined as] actions involving any of the following:
(a) access to information systems; (b) information system interference; (c) data interference; or (d) data interception, where such actions are not duly authorised [...]". Source: Forskrift om restriktive tiltak mot cyberangrep. (2021). Section 6, annex A, article 1, paragraph 2. *Forskrift om restriktive tiltak mot cyberangrep* (FOR-2021-05-11-1459). Lovdata. https://lovdata.no/dokument/SF/forskrift/2021-05-11-1459

to access one or more other organisations. A third-party attack can be combined with a supply-chain attack, but the two methods are in no way interdependent. Simply put, whereas a supply-chain attack targets a specific technology, a third-party attack targets the entire vulnerability surface of an organisation.

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

Destructive attack is a term generally used to refer to cyberattacks designed to destroy or sabotage an organisation's operations. This type of attack is typically carried out using malware that permanently deletes or corrupts data, and has a high potential for harm. Destructive cyberattacks are generally used in sabotage operations. **Disruptive attack** is an attack where, contrary to destructive attacks, the ensuing damage is a consequence rather than an objective. Examples of disruptive attacks include cyberattacks with ransomware. Destructive cyberattacks are generally more difficult to carry out than disruptive cyberattacks, as the physical or logical destruction typically demands in-depth knowledge and a thorough understanding of how the system works.

Denial-of-service (DoS) attack is a term used to describe an attack designed to deny, disrupt or hinder access to a service, server or network. When a botnet is used to flood a computer system with traffic, this is referred to as a distributed denial-of-service (DDoS) attack.

Digital fraud is a collective term for various malicious acts carried out on digital platforms with an view to manipulate, defraud or steal from individuals or organisations. It is the use of technology that separates digital fraud from other types of fraud.

Doxxing/doxing is a term used to refer to the publishing of personal or sensitive information about a person or organisation.

Vishing, or **voice phishing**, is a type of phishing where cybercriminals use phone calls (and potentially voice technology) to manipulate their victims into disclosing sensitive information.

Social engineering is a manipulation technique that exploits human weaknesses to gain access to private information, assets or other resources. Rather than the victim's inclination for criminal behaviour, it is often underlying factors such as urgency, stress, slip-ups, mindlessness or lack of training that enable malicious actors to succeed with social engineering.

Deepfake is a term used to designate synthetic media content (image, video or audio) that replicates or digitally alters locations, objects or living creatures but is presented as genuine. Deepfakes can e.g. be used to make a political figure appear to say something he or she has never said, generate video content

of a real person who is being kidnapped, but with the voice and likeness of another person, or show examples of apparent climate change in natural surroundings that has actually never happened. Deepfakes are generated using artificial intelligence tools including machine learning and deep learning.

Child sexual abuse material (CSAM) is a term used to refer to depictions of sexual abuse of children or depictions that sexualise children under the age of 18.[144]

Synthetic child sexual abuse material is a collective term for all material (photo, video, text etc.) that contain sexual abuse of children or in other ways sexualise children, and that is made using generative artificial intelligence.

Hybrid means is a term used to designate the combination of methods and approaches used by state actors who want to harm other states by other means than armed conflict to support their own strategic objectives. Examples are covert influence operations and the spreading of disinformation seeking to destabilise democracies and weaken the population's trust in key institutions. This way, authoritarian regimes can seek to create chaos or influence political decisions in another country.[145]

Miscellaneous

Complexity is a term used to describe systems with many interdependent elements and relationships, in which the interplay is non-linear and hard to predict. This results in characteristics and behaviours that cannot be explained by summing up the parts of the system. Organisational complexity arises when responsibility is fragmented and the organisation opaque.

Trigger is a term used to refer to events, statements, observations and similar that can trigger a process. Examples include wars and conflicts, sporting events, referendums and award ceremonies.

Complex or hybrid threats is a term used to refer to a situation where actors, e.g. states, use all the means available to them to achieve their goals. The methods may e.g. include influencing, coercion and physical harm to cause disarray in the population, undermine the sense of solidarity, manipulate the interests of other states, weaken democratic institutions and influence people's freedom of action. This typically takes place through covert action to avoid open conflict.

---

144 Norwegian Penal Code. (2025). Ch. 26, section 311. *The Penal Code* (LOV-2025-06-20-86). Lovdata. https://lovdata.no/dokument/NL/lov/2005-05-20-28/KAPITTEL_2-11#%C2%A7311

145 Parliamentary White Paper no. 13 (2024–2025). *Forebygging av ekstremisme: Trygghet, tillit, samarbeid og demokratisk motstandskraft.* Ministry of Culture and Equality. https://www.regjeringen.no/no/dokumenter/meld.-st.-13-20242025/id3092713/?ch=3

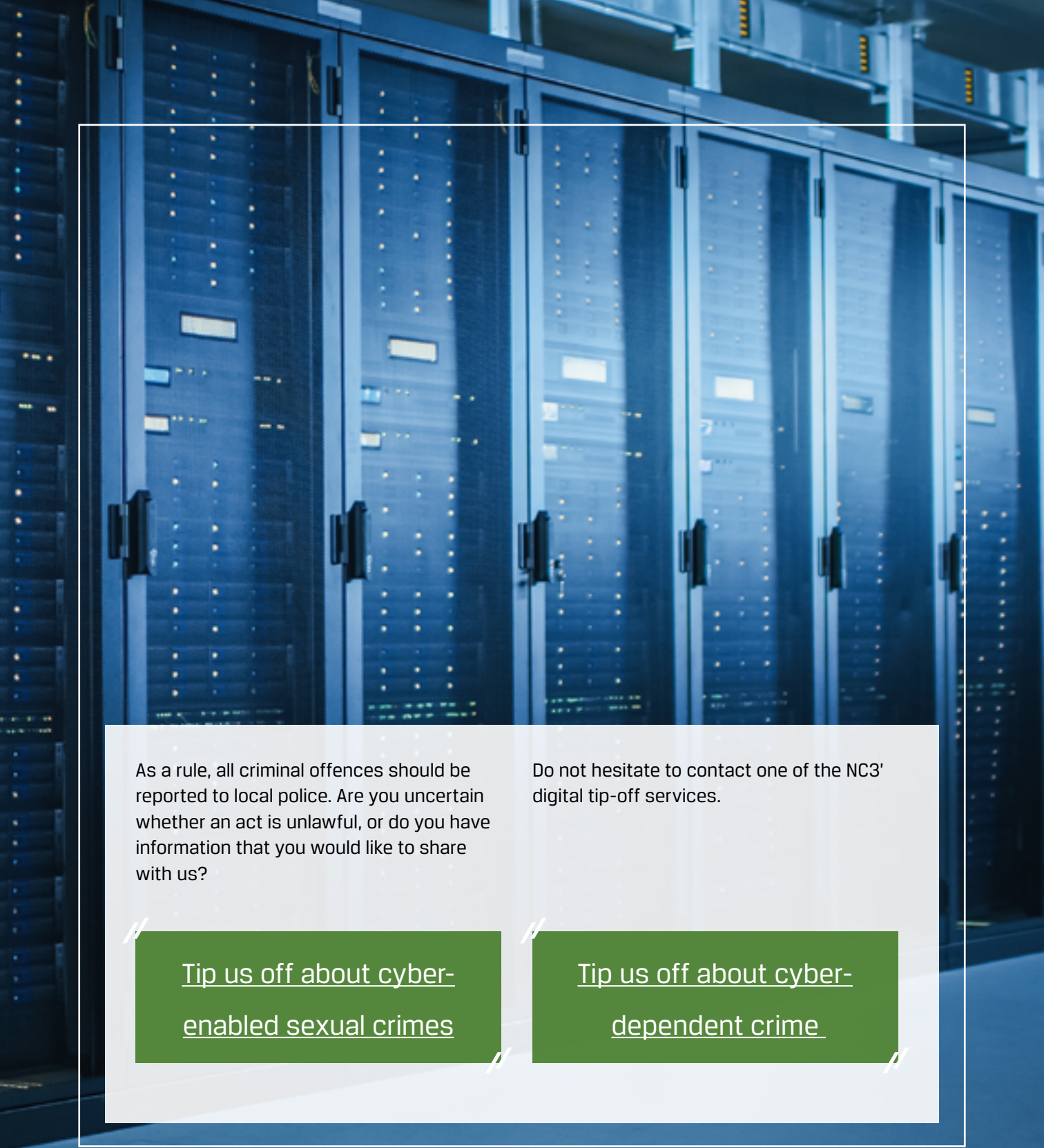
Security is in this report taken to mean the protection of data and computer systems from deliberate threats such as hacking and malware, whereas the term **safety** designates the protection of humans from accidental harm or risk.

Charts and illustrations

The task of the police is to protect people, property and public interest, and to defend all lawful activity and protect society against whatever threatens public safety. The police's task is also to prevent crime, uncover and stop criminal activity and bring offenders to justice.

The NCIS is the national unit for combating organised and other serious crime. It is also the national contact point and coordinating unit for international police cooperation and is responsible for the police's national intelligence production.

The National Cybercrime Centre (NC3) at the NCIS is mandated to combat cyber-dependent and cyber-enabled crime, in the latter case with a particular view to child sexual abuse. The NC3 holds specialist expertise and skills in initial cybercrime investigations. The department is responsible for preventing, averting and combating technology-driven crime, particularly cyber-dependent crime and online child sexual abuse.



As a rule, all criminal offences should be reported to local police. Are you uncertain whether an act is unlawful, or do you have information that you would like to share with us?

Do not hesitate to contact one of the NC3' digital tip-off services.

Tip us off about cyber-enabled sexual crimes

Tip us off about cyber-dependent crime

Photo: Shutterstock

POLITIET
KRIPOS

National Criminal Investigation Service NCIS (Norway)
Postal address: PO Box 2094 Vika, NO-0125 Oslo
Street address: Nils Hansens vei 25, 0667 Oslo

Contact: +47 23 20 80 00 / kripos@politiet.no

Front page photo: AI-generated