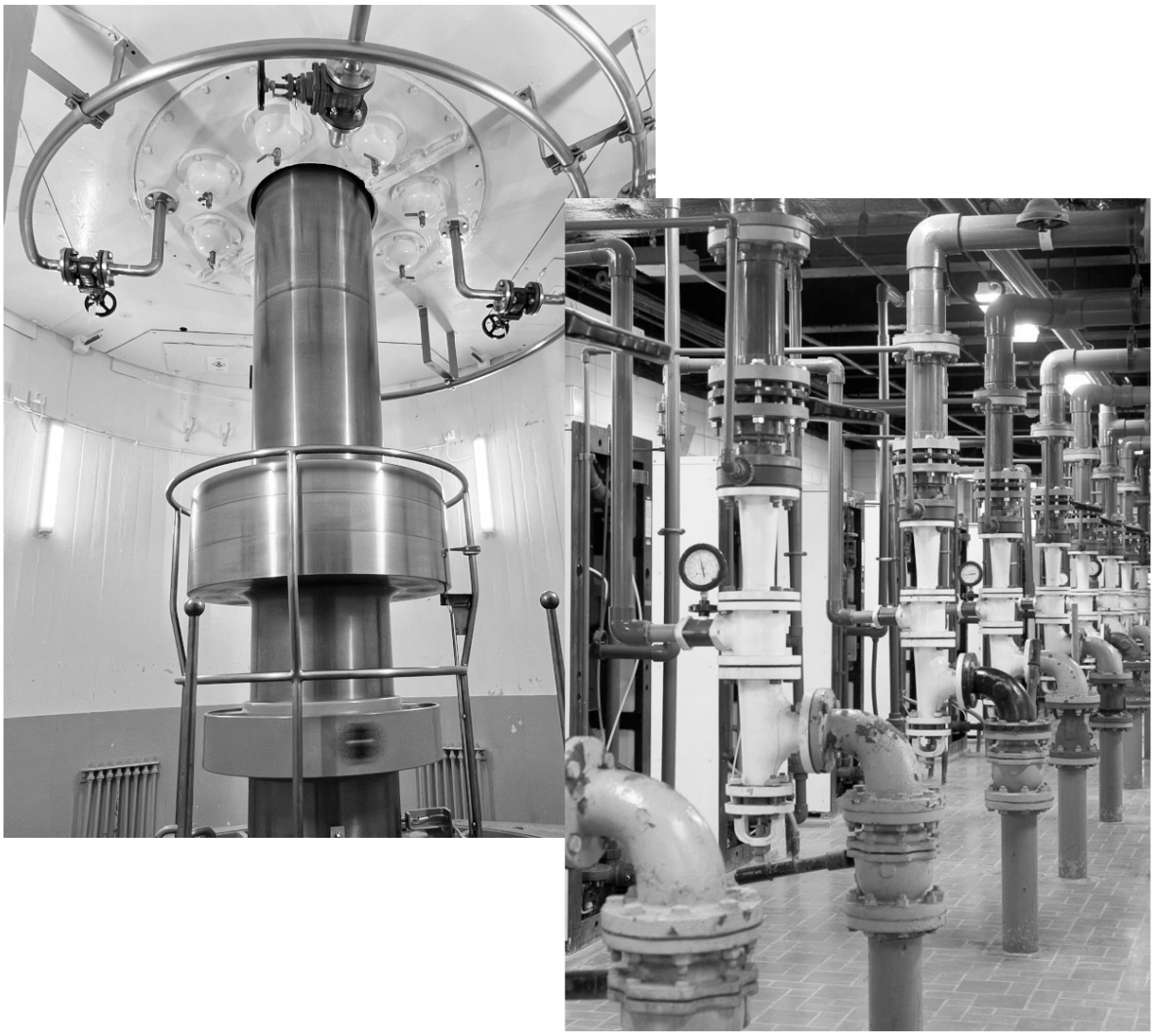
kraftCERT infraCERT



Threat assessment

2026

Contents

1 Threat assessment 2026

All organisations are exposed to threat activity. In IT, this means attempts to gain entry through well-known techniques such as phishing and abuse of legitimate tools. In OT[1] it means reconnaissance of exposed services, open ports, and poorly secured equipment.

The power and petroleum sectors are well-regulated sectors with mandatory baseline security in OT, but attacks in IT can still have consequences for OT through functional dependencies. Poorly secured OT systems without equivalent barriers are more exposed to direct attacks.

1.1 Key assessments

Criminal actors are the most likely attackers against organisations in our sectors.[2] It is almost certain (>90%) that the majority of attacks will exploit well-known techniques — exposed services, phishing, and abuse of legitimate tools — as the primary entry point.

It is likely (55–70%) that attacks against IT systems will produce operationally disruptive consequences for control systems where IT and OT are functionally interdependent. Isolation and shutdown of OT as a defensive measure is in itself sufficient to affect production.

It is unlikely (15–20%) that we will see successful destructive cyber attacks against industrial control systems in the near term among KraftCERT's members. Such attacks require detailed target knowledge, circumvention of multiple security layers, and sustained resource investment over extended periods.

Attackers will increasingly use the organisation's own legitimate tools to operate undetected and move through the network. In the IT zones, it is highly likely (75–85%) that internal legitimate tools are used for exfiltration and effect.

It is highly likely (75–85%) that all types of threat actors will use AI[3] to increase the pace and volume of attacks. AI reduces the production time for malware and makes scanning and phishing more scalable. AI gives actors faster working methods — not substantially new capabilities.

It is almost certain (>90%) that Russian-backed hacktivists will attempt attacks against vulnerable, internet-exposed infrastructure in Norway. It is plausible (25–40%) that they will achieve operationally disruptive effect against control systems with baseline security in place. It is highly unlikely (<10%) that Russian-backed hacktivists will achieve destructive effect, as they lack the target knowledge and technical resources to circumvent safety systems.

1.2 Uncertainty, method, and time horizon

The data basis for threat assessments in this field is weak or absent, and this is a general problem shared by both open and classified assessments. Statistics and trend descriptions relating to cyber attacks are consistently unreliable, poorly representative, and there are very many unsubstantiated claims. KraftCERT's assessments are based on knowledge, experience, observations, and critical reading and analysis of external reports, synthesised through analytical work. Where uncertainty is particularly high, this is indicated in the text.

[1] Operational technology
[2] Power, petroleum, water and wastewater, industrial production
[3] Artificial intelligence

2 Framework for understanding and use

2.1 Purpose and scope

Threat Assessment 2026 describes trends, threat actors, and attack types that KraftCERT considers most relevant to our sectors. The assessment covers actors' intent, capability, and opportunity, but does not address technical details, individual threat actors, or comprehensive vulnerability and consequence assessments.

The report does not include recommendations for specific measures. These will be developed and published in the Mitigation Package 2026.

The report looks 2–3 years ahead, with the near term assessed as approximately one year. For industrial control systems, longer time horizons are considered. The assessments are not universally applicable and must be read in the context of each organisation's own vulnerabilities and exposure.

2.2 About KraftCERT

KraftCERT is the operational sector response environment for the power and petroleum sectors, with membership also encompassing the process industry, the water and wastewater sector, and energy recovery. KraftCERT has members in both Norway and Iceland.

KraftCERT serves as both an ISAC (Information Sharing and Analysis Center) and an IRT (Incident Response Team) for our members. We provide support during cyber incidents and disseminate relevant and verified information about vulnerabilities, threats, and attacks.

KraftCERT is part of the national emergency preparedness structure, and collaborates with both private and public actors nationally and internationally.

KraftCERT is a member of the Forum of Incident Response and Security Teams (FIRST) and is a certified IRT in Trusted Introducer.

2.3 Probability terms, applicable from 2026

KraftCERT uses fixed terms to describe how likely it is that an event or development will occur. The terminology follows the Intelligence Service's national standard, which has been revised since our previous threat assessment in 2025.

Probability level	Percentage	Description
Almost certain	>90%	All indications point to this
Highly likely	75–85%	There is very strong reason to expect
Likely	55–70%	There is good reason to expect
Possible	45–50%	There is no balance of probability
Plausible	25–40%	There is limited reason to expect
Unlikely	15–20%	There is very limited reason to expect
Highly unlikely	<10%	No reason to expect

3 Situational overview

"We must accept that the world order as we knew it is dissolving", writes the head of the Intelligence Service in Fokus 2026[1]. The situational picture will be shaped by familiar threats in an increasingly unpredictable environment. Opportunism and economic gain remain the most important drivers behind the majority of attacks, but state threats must also be taken seriously. Espionage is part of the new normal. Digital and physical dependencies are increasingly being used as instruments of pressure[1][2].

Russia is known. China is known. What is new in 2026 is that our most important ally has become a source of uncertainty.

3.1 Cybercrime

Cybercrime is the most persistent and likely threat. Criminal actors are opportunistic and economically motivated[3]. Multiple simple attacks against many targets typically yield a greater total return than a small number of complex operations. Commercialisation, division of labour, and reuse of tools lower the barrier to entry and enable an increase in the number of attacks with limited effort[3]. Stolen data and valid access credentials are key commodities in a criminal economy where specialised actors sell on initial access to compromised systems[4]. Such access can subsequently be exploited for extortion, fraud, and further attacks[4].

3.2 State threats

Russia and China are the most relevant state-level threat actors for KraftCERT's members. The intelligence and security services[4] describe in their open assessments that both states have the intent and capability to conduct operations against Western targets, including Norway[1][5]. Iran and North Korea are assessed as less relevant to our sectors. Russia and China are addressed in greater detail in chapter 6 on Nation-states(s. 14).

It is highly likely (75–85%) that the war in Ukraine is the primary driver of Russian interest in Norway, as part of the Western bloc and as a supplier of power and petroleum to Europe. The High North and alliance politics are the most important long-term factors. Organisations with ties to Ukraine support will face a higher threat level than others[1].

Espionage is part of the normal state of affairs. State actors collect intelligence and establish access in peacetime to remain prepared for a range of possible developments[1]. Critical infrastructure, digital dependencies, and vulnerabilities in Norwegian digital infrastructure are sought-after targets for intelligence collection[5]. Apparently innocuous or fragmented information can, over time, yield insight into systems and interconnections that enables the planning and execution of attacks. It is the totality that determines the value, not any individual data point.

The Intelligence Service draws particular attention to mapping of infrastructure along the coast and on the seabed, and specifically identifies fibre-optic cables and gas pipelines as concrete targets[1]. Russia has dedicated units for such operations, and the Intelligence Service refers to them openly for the first time this year. Such mapping activity may also support sabotage[1].

Sabotage is assessed as a possible and primarily physical threat against KraftCERT's members. The most likely targets are property and logistics infrastructure related to support for Ukraine. In 2026, PST uses civil infrastructure as its target framework where it previously used critical infrastructure, without specifying what the term encompasses[5].

[4] The Intelligence Service (E-Tj), the Police Security Service (PST), the Norwegian National Security Authority (NSM)

3.3 Strategic uncertainty and dependencies

The stabilising role of the United States has diminished, and this affects the threat picture on multiple levels.

The cost of breaching international norms is declining. The Intelligence Service describes a global shift towards interest- and power-based politics in which international cooperation is weakening[1]. The United States' changing relationship with Europe is both a symptom of and a driver behind this shift, and reduces the risk calculus for Russia and other actors weighing action against European infrastructure. For our sectors, this means that assessments previously resting on the assumption that detection or diplomatic response would deter must be reconsidered. The thresholds are under pressure.

It is possible (45–50%) that dependency on American cloud services will be used as a political instrument of pressure, for example in the event of a crisis in the relationship between the United States and Europe. Norway has a high market concentration in such services[6]. In 2025, the United States imposed sanctions against an ICC[5] official that resulted in his being cut off from Microsoft's services[7]. More recent American strategic policy documents simultaneously describe the protection of American technologies, data centres, and supply chains as a strategic resource, as well as the use of private offensive cyber capability[8].

Threat perception is shaped by the wrong examples

Primitive attacks and unsubstantiated threats generate a major propaganda effect when amplified by authorities and the media.

The attack on a dam connected to a fish farm in Bremanger in April 2025 illustrates this. The attack was unsophisticated and the facility is in no way critical infrastructure, but PST's public remarks at Arendalsuka and NSM's national alert gave the pro-Russian group behind the attack far greater attention than they could have achieved on their own.

In February 2026, claims of "threats against the Nordic energy sector" generated massive media coverage. There was no concrete threat. Swedish authorities and media were unclear in their communication, but Norwegian newsrooms immediately amplified the story.

A recurring pattern is that target selection is rationalised after the fact: when an attack has occurred, a rational intention to strike precisely that target — or a sector, or some broader construct — is constructed in retrospect. The reality is most often that the attacker exploited an available vulnerability, and that the target was chosen because it could be attacked, not because it was important.

Neither an attack on a dam nor unsubstantiated claims on social media is a measure of how vulnerable critical infrastructure is or how serious the threat landscape is.

[5] International Criminal Court

4 Threats against industrial control systems

OT is the core systems for KraftCERT's members. IT supports operations, but it is the effect on the control systems and on service delivery that determines how serious a cyber attack is for our sectors.

This chapter structures the OT threat by effect category: nuisance attacks, disruptive attacks, and destructive attacks. The distinction is analytically important because the three categories carry different probabilities, place different demands on the attacker, and affect different organisations differently.

OT systems vary in security maturity depending on sector and function. They are subject to regulations and guidelines based on criticality that govern the design of security measures, barriers, and infrastructure.

4.1 Nuisance attacks

A clear trend in recent years is simple attacks from opportunistic threat actors such as Hacktivists and so-called faketivists, who, on the basis of geopolitical events, target vulnerable and accessible OT systems. These actors operate systematically by identifying internet-exposed devices such as PLCs[6], HMIs[7], or other OT components with inadequate baseline security, and attacking them. The attacks against Israeli Unitronics devices in the autumn of 2023, carried out by Iran-affiliated hacktivists, illustrate this approach. Common to all affected systems was that they were directly accessible from the internet and lacked fundamental OT security[8].

It is almost certain (>90%) that Russian hacktivists will continue to attack vulnerable, internet-exposed OT systems. These actors have demonstrated an interest in targeting OT systems both across Europe and in Norway. Systems lacking baseline security are particularly exposed to the simple attack techniques employed by hacktivists.

It is plausible (25–40%) that hacktivists will achieve operationally disruptive effect from attacks against simple, internet-exposed OT systems. They seek simple, vulnerable targets, and when a system is compromised, process functions are manipulated opportunistically. The actor groups are active on social media, where they publish documentation from compromised systems and promote claims about attacks. These groups act largely in response to geopolitical events and operate in political grey zones. OT systems that comply with baseline security requirements under applicable regulation and guidelines are robust against this type of actor.

[6] Programmable logic controller
[7] Human-machine interface
[8] https://claroty.com/resources/reports/analyzing-cps-attack-trends

Nuisance attacks: attack opportunity follows the level of security.

Organisations with baseline security in place — typically those under effective sector regulation — will experience this as a noise problem. For organisations lacking an equivalent level of security, the same attack is the most likely and most tangible threat they face.

This is a choice at two levels: the choice the organisation makes regarding its own security posture, and the choice authorities make about what requires regulation. Facilities of significance to power supply or petroleum deliveries are regulated and therefore minimally exposed to this type of attack.

Outside regulated environments, many smaller systems exist with inadequate security where an attack would primarily have consequences for the owners — from wind farms to gravel contractors.

4.2 Disruptive attacks and operational disruption

Disruptive attacks aim to interfere with an organisation's service delivery. This can be achieved through direct attacks against control systems, or indirectly by attacking support systems necessary for operations. Other attacks may cause the same effect.

It is likely (55–70%) that threat actors will carry out attacks with consequences severe enough to produce an operationally disruptive effect. It is the organisations' uncertainty about the extent of the attack that leads to preventive shutdowns or isolation. Operationally critical components and processes within the OT zone may be forced into shutdown as a consequence of an attack in the IT zone. Isolation is an important method for preventing propagation into secure zones, while process shutdown is often a safety measure designed to prevent unwanted physical consequences — both give the attack a real operationally disruptive effect. Consequences can range from brief operational interruptions to prolonged production stoppages.

The Jaguar Land Rover attack (JLR)

An IT attack in August 2025 caused Jaguar Land Rover a prolonged operational shutdown[9]. Media coverage could give the impression that OT was compromised in the attack, but the reality is that both OT and the associated production systems and facilities were deliberately taken offline to minimise risk. In addition, many sub-suppliers were directly affected by the shutdown.

This is an example where the significant interdependencies between IT and OT produce a longer disruptive effect. Several of the purported OT attacks described in the media and on social media are not attacks directly against OT devices or infrastructure. This is a conflation of effect and vulnerability that can lead to a focus on fixing the wrong problem.

It is highly likely (75–85%) that ransomware attacks against IT systems will produce indirect effects, including operational disruption. Such attacks can trigger defensive measures such as isolation

or shutdown of OT and production to prevent further escalation. There are numerous functional dependencies between IT and OT that a ransomware attack can affect, and which may compel the organisation to carry out shutdown as a risk-reduction measure.

It is unlikely (15–20%) that attackers will succeed in carrying out direct denial-of-service attacks against OT equipment. Such devices are concealed behind multiple layers of security measures including segmentation and access controls that must be circumvented, or require physical access. The exception is unsecured and vulnerable equipment connected directly to the internet.

It is likely (55–70%) that nation-state actors will conduct disruptive attacks against organisations in a heightened security-political situation, such as in the lead-up to war. In the event of major security-political changes, threat actors may be particularly interested in exploiting all possible forms of dependencies between OT and IT systems.

> ***Operational disruption: caused by the defence, triggered by the attack***
>
> A cyber attack does not need to reach OT to affect operations. It is sufficient for the situation to be unresolved. At the same time, not all operational disruptions are equally serious. KraftCERT distinguishes three levels:
>
> - Disconnection: Shutting down communication between the OT zone and the IT zone is a defensive measure, not a sign of compromise. The facility continues to deliver, but without support systems and monitoring from the IT side.
> - Island operation: More intrusive. Production units operate independently of one another, without central coordination.
> - Shutdown: The most intrusive measure, either as an active decision by the organisation, or triggered automatically by safety systems designed precisely for this purpose: to bring the process to a controlled stop before the situation escalates.

4.3 Destructive attacks

Destructive attacks aim to inflict physical damage on infrastructure, equipment, the environment, or people — damage that cannot be remedied through recovery operations.

It is unlikely (15–20%) that we will see successful destructive attacks carried out against OT systems during the coming year. Destructive and targeted attacks against OT systems are extremely resource-intensive and technically demanding to carry out. Such an attack requires the threat actor to be capable of manipulating a broad range of security mechanisms and bypassing multiple layers of barriers. Where a process is coupled to safety systems, the complexity increases further. Deep insight into and detailed knowledge of the specific OT system and its relationship to the physically controlled processes is required in order to circumvent interlocks.

Malware with destructive effect in OT systems is extremely resource- and time-intensive to develop, test, and — above all — deploy with sufficient precision against a selected target. Such an operation requires detailed planning and target knowledge, the involvement of diverse specialist communities, and tailored attack techniques and tools for each individual target, since each target is unique. The malware used must be adapted to the vulnerabilities and attack surfaces the threat actor chooses to exploit. Vulnerabilities and attack surfaces change their exposure throughout the system's lifetime as weaknesses are closed and countermeasures are implemented. This progressively narrows the threat actor's window of opportunity.

5 Artificial intelligence (AI) in the threat landscape

AI is changing the pace of attack development, but not yet the fundamental distinctions in the threat landscape. This chapter treats AI as a cross-cutting factor; its specific manifestations are addressed under Threat actors and Techniques.

It is highly likely (75–85%) that AI will increase attack volume, particularly from less advanced actor types. Scanning, phishing, malware production, and content tailoring become faster and cheaper. Resource-limited groups such as hacktivists gain scaling capability without gaining improved technical capability. The near-term effect is quantitative, not qualitative. It is very difficult to predict how much volume will increase. Both how quickly attackers adopt new techniques, and how quickly defenders derive benefit from their own AI tools, remains uncertain.

It is highly likely (75–85%) that AI will expand intelligence collection against KraftCERT's members. Both state actors and criminal enablers use AI for this purpose. The systematisation and correlation of open-source information is a task AI handles well, and information that previously required manual effort is now accessible and manageable at a scale that can expand attackers' target selection. This applies particularly to apparently innocuous or fragmented information that can yield insight to an attacker when aggregated over time.

It is likely (55–70%) that AI use will become an attack surface within KraftCERT's members. As organisations adopt AI tools and AI agents, new entry points and new opportunities for lateral movement emerge within an attack. AI services that process email are vulnerable to covert commands, AI agents with elevated privileges can be compromised to achieve a deeper foothold, and shadow AI creates exfiltration opportunities outside the organisation's control. Here AI is simultaneously a vulnerability for the defender and a tool for the attacker. This assessment carries uncertainty — both internal and external AI have a short track record and have been little tested against real-world attacks.

It is plausible (25–40%) that attacks will be carried out by AI agents alone in the near term. The execution phase and certain decision thresholds still require human judgement, particularly in attacks against well-secured targets. The requirements for target knowledge, resource investment, and access that distinguish noise from serious attacks remain unchanged. This assessment carries uncertainty, in part because the defensive thresholds it rests on may themselves be challenged by the organisations' own AI.

It is possible (45–50%) that interaction between AI agents will become an attack vector in its own right in the long term. When an organisation's own AI agents and those of its suppliers begin to interact directly, trust relationships are created that an attacker can exploit without needing to compromise the agents themselves. Supply chain attacks could then become a form of LotL[9] in the same way that an unmonitored remote access connection is today. The uncertainty lies primarily in whether organisations will be able to adopt the technology with security built in from the outset.

AI increases the pace of the race defenders face, and attackers' methods are becoming faster and easier to develop. Organisations that digitise without control over new exposures expand the attackers' room to manoeuvre.

[9] Living off the Land

6 Threat actors

6.1 Overview

Behind the threat picture described in Situational overview, actors operate within an ecosystem of services, tools, and collaboration. The model illustrates how different actor types (enablers, criminals, hacktivists, and state actors) utilise or procure services such as access credentials, malware development, reconnaissance, and assistance with or execution of attacks. The model is intended to show how this grey or dark market enables attacks including espionage, extortion, pre-positioning, and direct sabotage. KraftCERT assesses that the vast majority of threat actors, regardless of type and motivation, primarily select targets based on available opportunity.

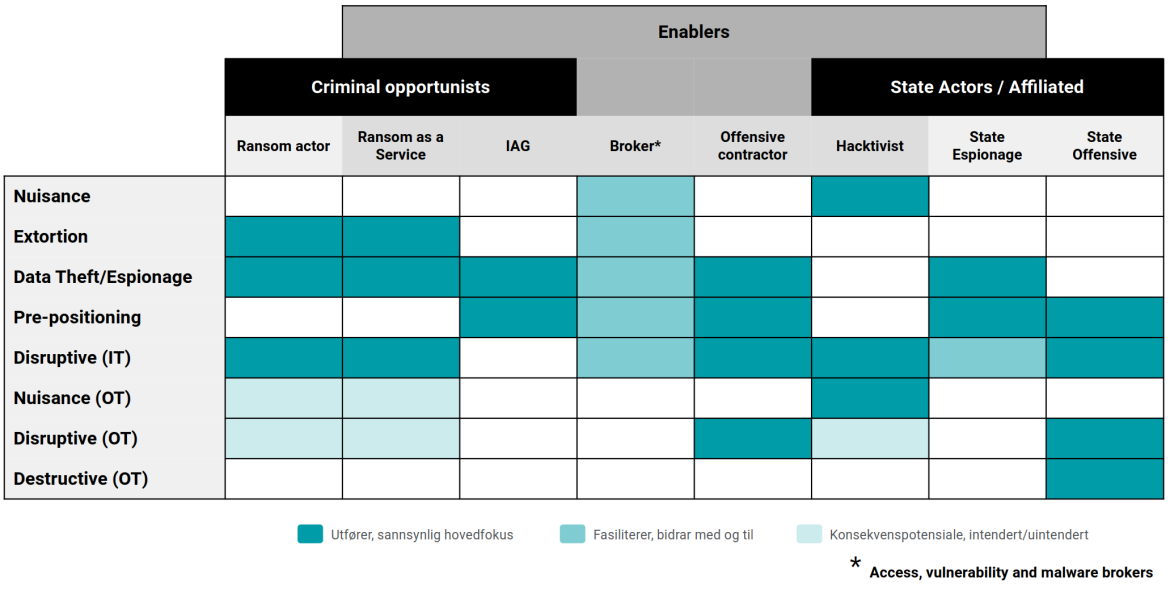


Figure 1: Relationship between actors, services, and attack types

6.2 Enablers

There is a large market of actors who facilitate attacks on behalf of others. These actors do not themselves conduct attacks directly against targets, but generate revenue by enabling such attacks for both criminal and mission-directed actors. This takes place on dark, or grey, markets.

6.2.1 Service providers

Both criminal and mission-directed actors purchase access to targets via vulnerabilities or login credentials. The buying and selling of vulnerabilities is an extremely lucrative industry. Specialised brokers such as Zerodium[10] operate in the grey zone between legal and illegal activity — they purchase unknown vulnerabilities from security researchers and sell them on, typically to intelligence agencies and law enforcement. In the criminal segment, older or previously used vulnerabilities are also traded on closed forums on the dark web, available to actors with far lower budgets than nation-states.

It is likely (55–70%) that tools used for espionage against nation-states are also used against organisations in our sectors. Tools such as infostealers migrate from state to criminal actors and vice versa.

[10] https://en.wikipedia.org/wiki/Zerodium

There are several so-called "grey zone actors"[11] who sell ready-made espionage tools to governments, which are then used to surveil journalists and human rights defenders by exploiting vulnerabilities in personal devices such as phones and computers.

AI is being used to map (collect and correlate) information about targets, and this has made such operations significantly easier and faster to carry out. KraftCERT has previously written about IAGs[fn:Inital Access Group]/brokers that collect and/or sell initial access to organisations, and the number of such groups has increased. We assess that this will continue to be the case going forward, both in the near and longer term.

6.2.2 Offensive contractors

It is highly likely (75–85%) that nation-state actors hire "hackers for hire" to participate in or independently carry out attacks[10][11]. These may be actors operating on the dark web or legitimate security companies in China, Russia, the United States, or Europe[12]. In China in particular, the line between state and commercial actors has nearly been erased, but both Russia and the United States make extensive use of contractors for security work, including offensive operations[8].

6.2.3 Insiders

Insiders who deliberately facilitate attacks have significant potential for harm to organisations, but this is a low-probability threat.

It is plausible (25–40%) that an insider will be coerced into carrying out or participating in disruptive or destructive attacks. An active insider in effect operations takes on considerable risk, particularly when the attack has a physical component. The actions leave traces that can be captured in logs and require the circumvention of security controls. The threat actor burns the resource an insider represents, so even though Russia's risk appetite appears to be increasing, the operational gain must be substantial to justify the use of this approach.

However, it is likely (55–70%) that a threat actor will attempt to recruit insiders to gather information for use in subsequent cyber operations. An established insider subjected to pressure or threats is a genuine source of information leakage, and it is this that makes insider recruitment attractive to threat actors.

Threat actors use social media, among other channels, in attempts to recruit insiders. The emergence of "crime-as-a-service" in the physical domain demonstrates that this occurs, and that it can take place in a more covert manner than traditional recruitment.

[11] Legitimate companies that buy from and sell to both legitimate actors and criminals

Insider threat: low, unknown, but real

The insider threat is real and carries significant harm potential, but the probability for any given organisation is nearly impossible to determine.

A review by FOI of European espionage cases[13] between 2008 and 2024 identified only 70 cases, none from Norway or Iceland. KraftCERT's own member survey shows the same pattern: 72% have not experienced insider incidents, while 77% have experienced unintentional errors with security consequences.

KraftCERT's research report on personnel exploitation[14] from 2025 notes that the field lacks a common conceptual framework and reliable indicators, making precise assessment difficult for all parties — including security authorities, KraftCERT, and the organisations themselves.

The analytically important distinction is between deliberate insider action and unintentional errors. These require different assessments and different countermeasures.

6.3 Criminal actors

Criminal actors will remain the most likely attackers against our members. Criminal actors are motivated by financial gain. They will use extortion, or sell the information they obtain. They constantly scan for technical vulnerabilities (see Direct technical access) and the number of actors seeking to gain access through phishing is growing (see Service providers).

Criminal actors regard our members as attractive targets. Almost all of our members are small or medium-sized companies, and actors view them as easier both to exploit and more likely to pay. Larger companies often have both a higher level of security and a policy against paying ransom [12]. The fact that energy in the United States is seen as a sector with high revenues and willingness to pay makes it reasonable to assume that some less sophisticated criminal groups believe the same applies to companies in Norway, even though there are many other significant differences between the petroleum and power sectors.

The number of reported ransomware attacks globally appears to continue increasing, while payouts are stable or declining. The reason is improved security practices in Western countries, and particularly in the Nordic region. In the longer term, this will lead to diminishing returns for ransomware actors, causing them to shift towards targeting markets that are less security mature.

Criminal actors who cannot exploit compromised access credentials or information themselves will sell or trade them in various arenas. This occurs across actor types and is an established part of the criminal economy.

It is plausible (25–40%) that law enforcement operations will have a lasting effect on cybercriminal groups in the long term. Authorities in both Europe and the United States have conducted numerous operations in the form of takedowns of criminal groups' infrastructure over the past year. Many actors nevertheless resume operations once they have rebuilt their attack infrastructure. It is difficult to apprehend individuals in groups that reside in countries without extradition agreements.

The number of criminal groups conducting attacks is growing. The reason is likely fragmentation resulting from law enforcement operations, and the fact that a larger share of criminal activity is being conducted online.

[12] Mitigation Package 2025 - Establish procedures for ransomware attacks (7413)

It is highly likely (75–85%) that suppliers to our sectors will be attacked by extortion actors. Smaller companies not subject to regulatory oversight will be particularly exposed, especially where awareness and knowledge of IT security is low. It is less likely that larger suppliers will be attacked, but attacks against these will have a significantly greater impact on the organisations that use them. Depending on the nature of the service, such companies will often have multiple and deeper direct access connections to the organisation, which can create greater uncertainty.

It is highly likely (75–85%) that larger suppliers will withhold information about cyber attacks, or share only the strict minimum required. Larger companies face greater reputational risk from attacks than smaller ones, and will attempt to control the narrative. KraftCERT has itself experienced this during incidents.

It is highly likely (75–85%) that threat actors will compromise targets via code available on the internet. Over the past year there have been numerous examples of GitHub repositories and packages included in JavaScript code[13] or Python packages[14] being injected with malicious code. This is a straightforward way for threat actors to establish a foothold inside an organisation, either directly or via a supplier. Such code repositories have in some instances been a source through which threat actors can obtain login credentials or steal information.

6.4 Mission-directed actors

Building attack capability is the most important long-term ambition for state actors. In the geopolitical competition, states seek the ability to strike critical targets belonging to adversaries. Mission-directed actors are primarily motivated by considerations other than the purely economic.

In the near term, however, the availability of attack opportunities is a more important factor in target selection than pursuing specific organisations, as demonstrated by the attack on Polish wind farms in 2025. Poor security of internet-exposed equipment gives attackers an opportunity to penetrate a sector that is normally difficult to compromise, and they choose to exploit this opportunity to achieve effects other than physical consequences — for example as part of a propaganda campaign designed to sow uncertainty.

6.4.1 Nation-states

Russia maintains the ambiguity between state, state-sponsored, and pro-Russian activity as a strategic instrument. It is almost certain (>90%) that Russia will continue to support, guide, and exploit hacktivists and pro-Russian groups for attacks against Norwegian infrastructure. KraftCERT's assessment of these actors is addressed in the chapter on Hacktivists.

It is unlikely (15–20%) that Russia will carry out attacks with destructive effect against Norwegian organisations. This assessment is unchanged from KraftCERT's analyses in 2023, 2024, and 2025. Targeted destructive cyber attacks against industrial control systems require substantial resources over extended periods and carry significant potential for conflict escalation. Although Russia appears to have a higher risk appetite, it still has many resources committed to the war against Ukraine, and it will therefore take time before it has built the capacity to carry out successful attacks against infrastructure of significance.

KraftCERT assesses it as plausible (25–40%) that Russia will conduct cyber attacks producing direct disruptive effect/operational disruption against our sectors in the near term. Although attacks against Ukraine continue, there is now a shift towards more espionage activity and fewer attacks with direct effect. The aim of such attacks in Ukraine is now to intimidate personnel in order to delay recovery, or to gather intelligence following kinetic strikes.

[13] https://en.wikipedia.org/wiki/Npm
[14] https://en.wikipedia.org/wiki/Python_(programming_language)

All nation-states with offensive capabilities will seek to build cyber attack capability. Nevertheless, we have seen few attacks with major effect, even in conflict situations. When conflict arises, states will use the means and opportunities available to them, regardless of actual effect potential. An example is Iran's attack on medical device manufacturer Stryker, which demonstrates that state actors also strike organisations peripheral to the ability to mount a defence.

Nation-state actors use openly available information about organisations in our sectors to identify vulnerabilities and plan attacks. The use of AI by both internal resources (ch. 7 Techniques) and contracted resources (ch. 6 Enablers) means that the scope of such collection has the potential to increase dramatically. Enhanced capacity to systematise and correlate such open-source information can create additional attack opportunities.

It is highly likely (75–85%) that Chinese actors will collect intelligence from our sectors. The collection may be directed at technological insight and software vulnerabilities that could provide access to Norwegian organisations or strengthen China's room for manoeuvre over time[1][5]. Chinese actors simultaneously seek to conceal both their methods and their affiliation[5]. This is achieved by using legitimate cloud services to conduct covert operations.

It is also likely (55–70%) that Chinese actors target the telecommunications industry through selected organisations and suppliers, and frequently attack network equipment (see Direct technical access) about whose vulnerabilities they have detailed knowledge or prior insight. The attacks will highly likely (75–85%) be conducted either directly against the organisations or through their supply chain. PST describes Salt Typhoon[15] as an example of Chinese actors having compromised vulnerable network devices at a Norwegian organisation[5]. This activity has not been observed in KraftCERT's sectors.

It is unlikely (15–20%) that China will conduct disruptive or destructive attacks against our sectors. The resource requirements are the same as for Russia, and China is not in direct conflict with Norway or Europe. Nevertheless, KraftCERT assesses it as possible (45–50%) that they will attempt to pre-position themselves for future attacks.

Iran and North Korea are assessed as less relevant threat actors for our sectors. Iran is given greater prominence in PST's 2026 assessment, but the target picture is primarily dissidents, critics, Israeli interests, and other Western targets[5]. Iranian hacktivists could, in an extreme scenario, attack Norwegian companies due to a perceived solidarity between Norway and the United States, but this appears plausible (25–40%). North Korea is more often relevant through cryptocurrency fraud and attempts to place North Korean IT developers inside Western organisations under false identities[5]. These are relevant threats at a societal level, but less central to our sectors than Russian and Chinese activity.

6.4.2 Hacktivists

Politically motivated hacktivists attempt to conduct attacks against their adversaries, or attempt to link more opportunistic targets to their political cause. The term hacktivism encompasses both nation-state-directed/supported/aligned actors and ideologically driven actors.

Hacktivists are loosely organised groups of individuals with an explicit declared intent to conduct attacks with a political agenda in service of a state or state-like insurgent group. They may be supported by nation-states, but this is not a requirement. There are also "fakitivists": state actors posing as hacktivists to avoid attribution.

Unlike the classical definition of a hacktivist as a purely ideological actor, hacktivists today select targets based on ongoing political and regional conflicts. The aim of the attacks is propaganda and to create unrest

[15] https://en.wikipedia.org/wiki/Salt_Typhoon

in the countries being targeted. A shift in target selection in response to geopolitical events is frequently observed, as seen following the attacks on Ukraine, Gaza, and Iran.

It is unlikely (15–20%) that domestic, ideologically driven actors will attempt to conduct cyber attacks against our sectors, such as local wind power opponents or climate activists.

It is highly likely (75–85%) that Russian-backed actors will carry out attacks against poorly secured infrastructure in Norway over the coming year. It is likely (55–70%) that pro-Russian hacktivists will attack weakly secured OT systems, but it is plausible (25–40%) that they will be able to carry out attacks against OT systems that are within well-regulated sectors or organisations that have baseline security in place.

It is highly likely (75–85%) that state-backed hacktivists receive assistance from state actors with both target selection and access to tools. Open access points — whether through vulnerabilities or access credentials — are the primary driver of target selection for hacktivists. AI means that even resource-limited hacktivist groups can scan and map more targets than before, without this translating into improved technical capability to carry out more sophisticated attacks.

7 Techniques

7.1 Unified Kill Chain

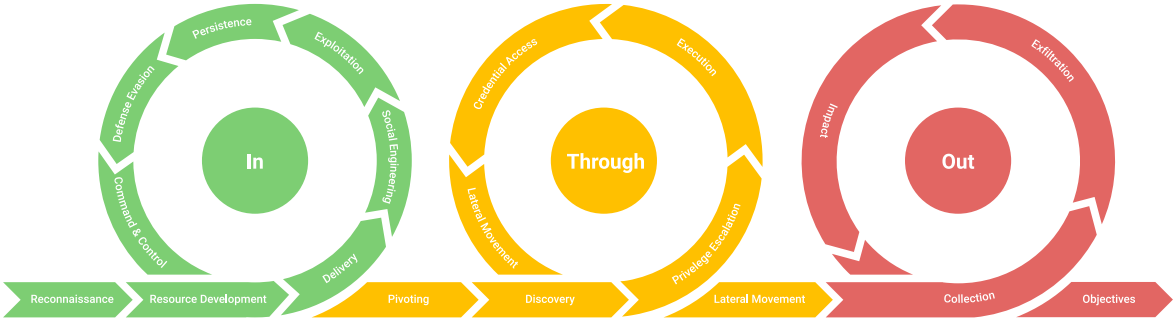


Figure 2: Unified Kill Chain (UKC)

Threat actors use many of the same techniques, regardless of who they are and what they want. This chapter describes the attack chain structured according to the Unified Kill Chain: access, movement, and execution. Access is about getting in, movement about spreading further without being detected, and execution about carrying out what the attacker came to do.

7.2 Access (In)

7.2.1 Reconnaissance and target selection

KraftCERT assesses it as almost certain (>90%) that mission-directed actors will scan all of our members' infrastructure to map devices, networks, and system details. Scanning is carried out as preparation for attacks, and is conducted by most types of threat actor. The purpose is to identify potential targets where compromise requires minimal resources, either for simple purposes such as propaganda or for long-term pre-positioning.

Such scanning is performed in an automated and large-scale manner, increasingly with AI support, and enables the identification of attack surfaces in exposed services, open ports, and technical vulnerabilities without directly attacking the target.

For more advanced threat actors, reconnaissance is closely linked to exploitation of known and unknown vulnerabilities, but even relatively simple actors scan for exposed equipment with default credentials.

7.2.2 Direct technical access

Exposed services will likely be the most important entry point. Remote access services, such as VPN or purpose-built services, and applications such as VNC[16] are visible when scanning as they are exposed to the internet. Both legitimate services such as Shodan[17], and threat actors actively scan all exposed internet services on a continuous basis.

It is highly likely (75–85%) that threat actors will attempt to compromise (I)IoT devices exposed on the internet, as these contain numerous vulnerabilities and are often unsecured. IoT[18] devices are

[16] Virtual Network Computing
[17] https://www.shodan.io/
[18] Internet of Things

frequently configured without active application of the organisation's security policies, or by suppliers of specialist services. Even where these are not directly connected to the organisation's network, the devices can be used as a pivot point or to gather information.

It is likely (55–70%) that vulnerabilities in perimeter equipment will be exploited by all types of threat actors. The proportion of successful compromises exploiting vulnerabilities has increased, and is carried out by mission-directed actors, criminals, and enablers alike. Actors exploit both known and unknown vulnerabilities, as well as so-called "bruteforcing"[19] techniques.

Google Threat Intelligence Group recorded just under 100 actively exploited zero-days in the period 2023–25, of which over 40 percent targeted exposed network equipment such as VPNs, firewalls, and routers. The market for such vulnerabilities is directly reflected in the attack patterns against perimeter equipment that KraftCERT observes in our sectors[15].

It is highly likely (75–85%) that threat actors will attack via cloud services. This applies particularly to web-facing and cloud services where legitimate users access functionality through a browser. Techniques such as ClickFix[16] combined with infostealers give attackers the ability to steal login credentials and session tokens in order to attack exposed services.

Figure 3: UKC - "In"

KraftCERT assesses it as highly likely (75–85%) that Chinese nation-state actors will attack equipment from specific vendors to the telecommunications industry by exploiting vulnerabilities they are familiar with. Mission-directed actors often possess in-house expertise and knowledge of vulnerabilities that are not publicly known. Chinese authorities have also enacted legislation granting them first right of access to all vulnerabilities discovered, in order to retain these in their tool repositories[17][18].

It is likely (55–70%) that AI will be used to develop attack malware for phishing and deepfake campaigns. Attackers exploit the fact that authentication of user accounts without phishing-resistant MFA[20] is often straightforward to bypass using phishing or bruteforcing. Ransomware groups have to a large extent automated such intrusion processes. This has both reduced the time such a compromise takes and increased the number of attacks it is possible to carry out.

It is highly likely (75–85%) that AI-assisted malware will, in the near term, significantly reduce the time an intrusion takes, and this applies particularly to "Malware-as-a-Service" (MaaS[21]). The development of AI tools has reduced the production time for malware, especially where it is purpose-built to exploit recently disclosed vulnerabilities obtained from advisories.

It is highly likely (75–85%) that attackers will, in the near term, attempt to exploit organisations' own AI tools as an entry point. Several organisations have adopted Copilot as a tool for processing incoming email, and these are vulnerable to covert commands invisible to the human eye that are processed by the AI service[19].

Threat actors will attempt to compromise remote access solutions in order to gain access to OT systems. Stolen credentials or the use of brute-force techniques can break weakly secured authentication mechanisms. Both in-house staff and suppliers through outsourced services have access via such solutions, and user accounts are of particular interest to threat actors.

19 Password guessing at scale
20 Multi-Factor Authentication
21 Malware-as-a-Service

It is highly likely (75–85%) that attackers will exploit vulnerable perimeter devices as an entry vector into OT zones. Targeted mission-directed threat actors scan specifically for vulnerabilities, particularly in equipment located at the perimeter of the OT zone, such as VPN concentrators, firewalls, and other services accessible from the internet or the IT zone. Actors have a window between when vulnerabilities are disclosed and when they are patched that can be exploited, and as noted, the time required for malware production is declining.

7.2.3 Attacks via the supply chain

KraftCERT assesses it as likely (55–70%) that attack attempts will occur through the compromise and exploitation of suppliers. Their trusted relationship with organisations is exploited for compromise via phishing. Note that such attacks may have unintended effects on the organisations concerned, leading to operational disruption due to uncertainty and the precautionary principle.

KraftCERT assesses it as highly likely (75–85%) that organisations in our sectors will be affected by threat actors' attacks on code repositories [20][21]. Development environments use both open code repositories such as GitHub, and pull in modules or libraries from the internet during development. If an attacker introduces malicious code into developer-written code, this creates opportunities for direct attacks.

Opportunistic actors attacking suppliers are looking for account credentials belonging to users with elevated privileges, particularly with access to customers' systems and infrastructure. Remote access is noted above, but access to customers' data or information is also of great interest. Such data is highly valuable because access credentials can easily be resold. Information about targets assessed as critical infrastructure can also have value in the interplay between criminal actors and Russian security services, where legal cover for criminal activity directed abroad can be exchanged for services or payment[22].

7.3 Movement (Through)

LotL[22] **is threat actors' preferred method of operation.** Most attackers make every effort to move unnoticed through security systems and interfaces without being detected. Legitimate tools also have access across zones, providing opportunities for both lateral movement between endpoints and movement across interfaces such as firewalls.

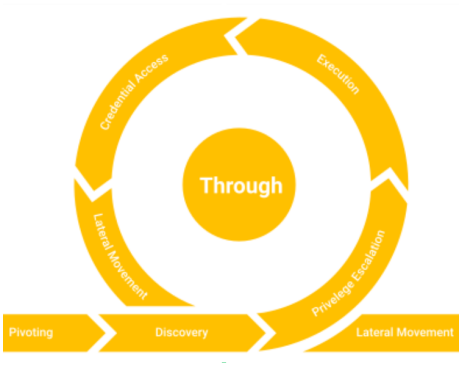


Figure 4: UKC - "Through"

Attackers use legitimate internet tools for command and control. These have outbound internet access and cannot easily be blocked by organisations without affecting normal internet usage.

It is likely (55–70%) that advanced actors will attempt to compromise AI agents in use within organisations to achieve a deeper foothold in the organisation's infrastructure. For example, a compromise of AI agents used for internal code development could give an attacker both insight and a straightforward means to deploy malware.

It is likely (55–70%) that threat actors will attempt to attack AI services to gather information prior to exfiltration[23]. This applies particularly where organisation employees have adopted "shadow AI"[23].

It is almost certain (>90%) that threat actors develop and use malware specifically targeting all types of operating systems. In addition, malware is developed against hypervisors such as VMware and Hyper-V, and container technologies such as Kubernetes, Docker, and similar platforms.

It is likely (55–70%) that attackers will exploit the absence of traffic authentication for lateral movement, both internally in the communication path between SCADA[24] and field devices, and in integrations used to exchange data between OT and IT systems. KraftCERT considers it possible (45–50%) that integrations over the internet are attacked directly, but we have not yet observed use of this technique.

It is highly likely (75–85%) that the use of legacy protocols constitutes an attack surface that threat actors can exploit, if they have already gained entry inside the OT zone perimeter. Several communication protocols have a low level of inherent security, as security was not part of the original design — including Modbus, Profibus, and Elcom. Advanced state actors such as Sandworm have demonstrated that they have, and continue to develop the capability to develop attack techniques targeting different OT technologies in order to compromise OT systems[24, s.1].

It is highly likely (75–85%) that Russian state actors have the capability to exploit vulnerable OT systems and communications protocols. Older OT systems are often impossible to update and lack security features, and contain numerous software and architectural vulnerabilities that threat actors will exploit for footholds, movement, and effect. If there are insufficient barriers and resilience built into the zones, this could be exploited by an attacker where the organisation lacks adequate baseline security.

It is likely (55–70%) that vulnerabilities in virtualised environments will be exploited by malware in the coming years. Virtualisation of OT infrastructure and the use of virtual devices and environments has increased considerably in recent years — including in OT. It is likely (55–70%) that OT systems, or systems connected to the control system, that are hosted in the cloud will be attacked in the same manner.

[22] Living off the Land
[23] AI use outside organisational control and policy
[24] Supervisory Control and Data Acquisition

7.4 Execution (Out)

Attackers use legitimate internet tools for data exfiltration. This is not new, but the proliferation of file-sharing and communication tools in use within organisations means it is difficult to monitor, both from the attacker's perspective and in relation to illegitimate use by the organisation's own users.

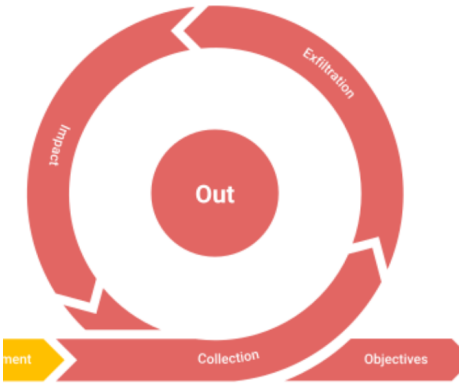


Figure 5: UKC - "Out"

In the near term, it is plausible (25–40%) that threat actors will carry out successful attacks executed by AI agents alone. It is however possible (45–50%) that parts of the execution phase will be carried out by AI agents with human oversight. As noted, extortion actors already operate with a high degree of automation, and with AI support this automation will extend to more stages of the attack chain. It is highly likely (75–85%) that AI is used directly in malware production.

It is unlikely (15–20%) that we will see ransomware developed specifically against OT equipment or systems during the coming year. Such systems are fundamentally different from standard IT systems, and it is therefore demanding to develop effective capabilities against the OT-specific components of those systems. It is simpler to deploy ransomware against the IT elements of such systems: the operating system or file system. The most recent known example of ransomware targeting OT is EKANS[25] from 2020.

Attackers have an extensive toolkit of wipers. Such tools can target virtually any type of equipment. Wipers are used to erase data, configuration, operating systems, and firmware, and have been used extensively in Ukraine. The malware used in the Polish incident also shares characteristics with malware used by Russian nation-state actors.

It is likely (55–70%) that OPC-UA as a communications technology will be incorporated into future malware targeting control systems. The use of OPC-UA[26] for communications and data exchange across zones in OT systems is a technology development driven by digitalisation and the evolution of "Industry 4.0"[27]. More OT systems and sectors will adopt this technology, which may result in a larger number of homogeneous solutions. This could provide threat actors with greater opportunity for lateral movement and access to more devices and networks where OPC-UA is in use and where authentication and traffic verification are inadequate.

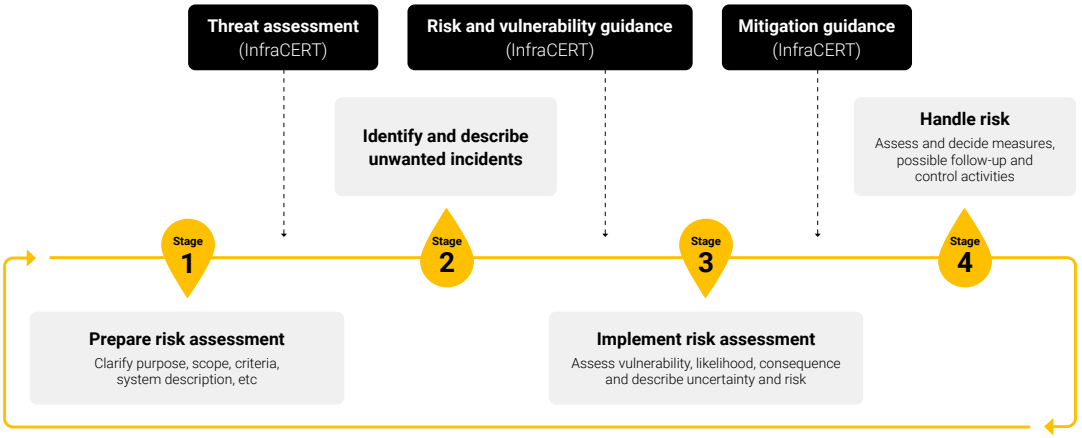
[25] https://malpedia.caad.fkie.fraunhofer.de/details/win.snake
[26] OPC Unified Architecture
[27] https://en.wikipedia.org/wiki/Fourth_Industrial_Revolution

8 About the report

8.1 Threat assessment and mitigation package

The threat assessment is followed up with a mitigation package for members in autumn 2026. It will provide practical recommendations and seek to answer how the threats can best be addressed. Together these can contribute to the organisation's risk and vulnerability analysis. Security is cheapest when built in from the start. New technology and new integrations expand the attack surface. The mitigation package provides concrete recommendations, but the most important advice can be given already now:

Security must be a dedicated consideration in all planning and development — not something added on afterwards.

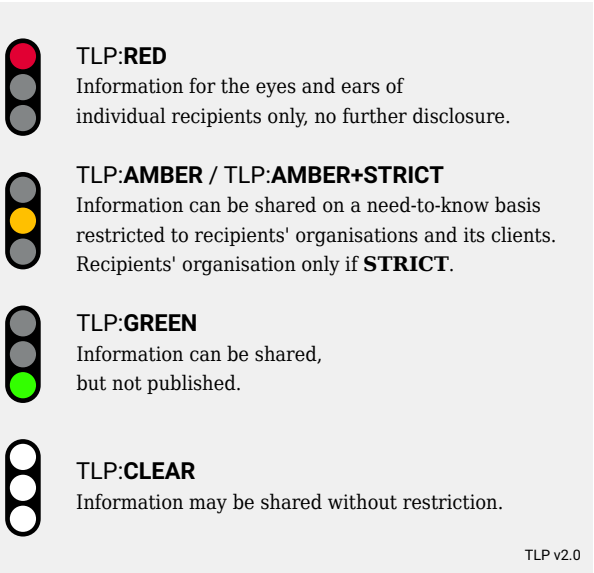


8.2 Traffic light protocol

KraftCERT/InfraCERT uses the traffic light protocol (TLP version 2.0) when sharing information to indicate how the information may or may not be shared further.

This document is classified as TLP:CLEAR. Disclosure is not limited.

Read more about the traffic light protocol at FIRST[28].



8.3 Changelog

Date	Version	Description
2026-04-30	1.0.0	First release

[28] https://www.first.org/tlp

References

[1] Etterretningstjenesten. *Fokus 2026*. Mar. 2, 2026. URL: https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-pa-norsk/Fokus2026%20-%20NO%20-%20Weboppslag%20v4.pdf.

[2] Forsvarets forskningsinstitutt. *Forsvarsanalysen 2025*. Feb. 17, 2025. URL: https://www.ffi.no/publikasjoner/forsvarsanalysen-2025.

[3] Politiet. *Cyberkriminalitet 2026*. Mar. 17, 2026. URL: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2026.pdf.

[4] Europol. *Steal, deal and repeat - Internet Organised Crime Threat Report 2025*. June 13, 2025. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf.

[5] Politiet. *Nasjonal trusselvurdering 2026*. Mar. 2, 2026. URL: https://www.pst.no/wp-content/uploads/2026/02/Nasjonal-trusselvurdering-2026.pdf.

[6] EPRS. *Cloud and AI development act*. Apr. 1, 2026. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/779251/EPRS_BRI(2025)779251_EN.pdf.

[7] The White House. *IMPOSING SANCTIONS ON THE INTERNATIONAL CRIMINAL COURT*. Feb. 6, 2026. URL: https://www.whitehouse.gov/presidential-actions/2025/02/imposing-sanctions-on-the-international-criminal-court/.

[8] The White House. *President Trump's CYBER STRATEGY for America*. Mar. 2, 2026. URL: https://www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf.

[9] CYFIRMA. *Investigation Report on Jaguar Land Rover Cyberattack*. Sept. 24, 2025. URL: https://www.cyfirma.com/research/investigation-report-on-jaguar-land-rover-cyberattack/.

[10] Chatham House – International Affairs Think Tank. *Holding state-sponsored hackers and other cyber proxies to account*. Apr. 20, 2026. URL: https://www.chathamhouse.org/2026/03/holding-state-sponsored-hackers-and-other-cyber-proxies-account.

[11] DeepStrike. *State-Sponsored Hacking: Global Trends and How to Defend in 2025*. Dec. 16, 2025. URL: https://deepstrike.io/blog/state-sponsored-hacking-apt-threats-2025.

[12] SpyCloud. *State Secrets for Sale: More Leaks from the Chinese Hack-for-Hire Industry*. July 1, 2025. URL: https://spycloud.com/blog/state-secrets-for-sale-chinese-hacking/.

[13] FOI Totalförsvarets forskningsinstitut. *"Spies Among Us": Espionage in Europe - A study on convicted spies in Europe 2008–2024*. Feb. 3, 2026. URL: https://www.foi.se/rest-api/report/FOI-R--5866--SE.

[14] KraftCERT. *Forhindre utnytting av personell - Prinsipper og tiltak*. Nov. 13, 2025. URL: https://www.kraftcert.no/filer/KraftCERT-utnytting-personell.pdf.

[15] Google Cloud. *Look What You Made Us Patch: 2025 Zero-Days in Review*. Mar. 5, 2026. URL: https://cloud.google.com/blog/topics/threat-intelligence/2025-zero-day-review.

[16] Microsoft Security. *Think before you Click(Fix): Analyzing the ClickFix social engineering technique*. Aug. 21, 2025. URL: https://www.microsoft.com/en-us/security/blog/2025/08/21/think-before-you-clickfix-analyzing-the-clickfix-social-engineering-technique/.

[17] Strategist. *China's vulnerability disclosure regulations put state security first*. Aug. 31, 2021. URL: https://www.aspistrategist.org.au/chinas-vulnerability-disclosure-regulations-put-state-security-first.

[18] Atlantic Council. *Sleight of hand: How China weaponizes software vulnerabilities*. Mar. 13, 2025. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability.

[19] CovertSwarm. *EchoLeak: The Zero-Click Microsoft Copilot Exploit That Changed AI Security*. July 7, 2025. URL: https://www.covertswarm.com/post/echoleak-copilot-exploit.

[20] The Register. *Two different attackers poisoned popular open source tools - and showed us the future of supply chain compromise*. Apr. 10, 2026. URL: https://www.theregister.com/2026/04/11/trivy_axios_supply_chain_attacks.

[21] Datadog Security Labs. *Learnings from recent npm supply chain compromises*. Oct. 30, 2025. URL: https://securitylabs.datadoghq.com/articles/learnings-from-recent-npm-compromises.

[22] Atlantic Council. *Unpacking Russia's cyber nesting doll*. May 20, 2026. URL: https://www.atlanticcouncil.org/content-series/russia-tomorrow/unpacking-russias-cyber-nesting-doll/.

[23] CSO Online. *Top 5 real-world AI security threats revealed in 2025*. Dec. 29, 2025. URL: https://www.csoonline.com/article/4111384/top-5-real-world-ai-security-threats-revealed-in-2025.html.

[24] CERT Polen. *CERT Polska Energy Sector Incident Report 2025*. Jan. 30, 2026. URL: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/.