Cyberwatch Finland

MAGAZINE 1/2026

Cybersecurity is Built by Small Actions and Management of Large Concepts

Our Aim is to Add Cyber Capabilities in the World

Cyberwatch Finland

CONTENT

Cyberwatch Finland
MAGAZINE 1/2026

Cyberwatch MAGAZINE

PUBLISHER
Cyberwatch Oy
Nuijamiestentie 5 C
Helsinki, Finland

EDITORIAL
Editor-in-Chief
Aapo Cederberg
aapo@cyberwatchfinland.fi

LAYOUT
PuulaMedia / Mari Riepponen

ILLUSTRATIONS
AdobeStock

PRINT
Scanseri Oy, Helsinki

ISSN 2490-0753 (print)
ISSN 2490-0761 (web)

Cyberwatch Finland

Do We Have Sufficient Cyber Threat Intelligence Capability?

The state of the world looks increasingly chaotic by the day — uncertainty is growing, the global economic crisis is intensifying, and military operations continue in the Middle East and Ukraine. Our ability to form a reliable strategic situational picture is becoming increasingly difficult. The media is reporting on each crisis separately, but the overall picture of an interdependent world is becoming increasingly harder to predict. The significance of cyber weapons in various crisis hotspots is growing, particularly with the rapid development of artificial intelligence. At the same time, the increased use of AI amplifies the volume of disinformation, easy analysis produces false conclusions, and the reliability of available data is weakened. Meanwhile, new cyber legislation and complementary EU regulation obliges companies' board members and operational management to acquire a sufficiently comprehensive situational awareness of the cyber world, so that they are capable of risk-based decision-making. A challenging situation — so what is the answer?

Our capacity to manage the overall picture must be improved. Understanding the cyber world still rests on the ecosystem formed by human activity, operational processes, and technology — and of course on understanding the methods of cyber threat actors. Considering all of this, a reliable and anticipatory situational picture that takes into account the information needs at different levels of the organisation needs to be formed. The information needs can be broadly divided into the strategic view required by the top management, the operational situational awareness required by the operational management, and the technical situational awareness needed by specialists. All of this requires reliable data and an improved capability to analyse it. Cyber threat intelligence has become invaluable. The key question is how to build a sufficient threat intelligence capability for an individual company or organisation — whether it must be kept in-house or whether it can be procured from an external service provider. This is an important decision point that requires careful consideration and an understanding of the information needs and cyber maturity of the organisation in question. But where does that understanding come from?

The obligation to conduct a cyber risk analysis is a useful tool, provided it is carried out thoroughly and grounded in an assessment of the organisation's current state — along with a comprehensive reflection on what kinds of cyber risks are directed at it, their likelihood, and their impact. One must be familiar with the cyber threat landscape and be able to monitor changes within it. At the same time, it must be possible to assess how physical and digital risk factors are interdependent — therefore a comprehensive risk analysis based on reliable information is needed. Information needs and the importance of reliable analysis are revealed during the process. At the same time, it inevitably leads to the conclusion that a reliable cyber risk analysis cannot be conducted without effective cyber threat intelligence.

Together with DNV Cyber, we will be publishing a Cyber Threat Intelligence Handbook later this spring. Its aim is to illuminate the broader landscape of cyber threat intelligence and to facilitate decision-making for your organisation. The publication will be freely available to all and has been produced as a result of indirect industrial cooperation with Lockheed Martin. One of the key objectives of this research and development collaboration is to increase the cyber competence of the Finnish society — and that is precisely what this handbook seeks to contribute to.

AAPO CEDERBERG
Managing Director
and Founder
Cyberwatch Finland

New Wave of Cybersecurity Regulation

In recent years, cybersecurity regulation in the EU has undergone a historic transformation. The original Network and Information Security Directive[1], which came into force in 2016, was the EU's first attempt to harmonise cybersecurity requirements – albeit with modest results. However, Russia's invasion of Ukraine in 2022, coupled with an acceleration in cyberattacks against critical EU infrastructure and the exposure of vulnerabilities in digital supply chains, forced legislators to fundamentally rethink their approach. The result has been a tsunami of cybersecurity legislation that organisations must have learned to manage simultaneously.

Over the past four years, several major pieces of cybersecurity legislation have been adopted or finalised in the EU, including the NIS2 Directive,[2] the Cyber Resilience Act (CRA),[3] the Critical Entities Resilience Directive (CER),[4] the DORA Regulation on digital operational resilience,[5] and the Cyber Solidarity Regulation.[6] As a result, there are new obligations, new supervisory structures and regulation extending deeper into companies' internal processes, management structures and supply chains.

New Cybersecurity Obligations Applicable in 2026

September 2026 marks a pivotal moment for organisations operating in the EU digital market, as the CRA's mandatory vulnerability and incident reporting obligations will come into force. These obligations apply to a wider range of organisations than many might expect.

What Is the Cyber Resilience Act (CRA)?

Unlike current EU digital legislation, which mainly applies to service providers and infrastructure operators, the CRA imposes cybersecurity requirements directly on products with digital elements. This means that almost every hardware and software product that can connect to the internet or other devices will be subject to the CRA. This includes routers, smart home devices, industrial sensors, mobile games, operating systems and many enterprise software. In order for such products to be placed on the EU market, they must meet the CRA's essential cybersecurity requirements, and the manufacturer's processes must comply with the CRA's vulnerability-handling rules.

Who Does the CRA Apply To?

The CRA does not only apply to large technology companies; it applies broadly to different organisations that manufacture products with digital elements or make such products available on the EU market as part of a commercial activity. The obligations thus apply to manufacturers, importers and distributors of products.

However, certain categories of products, such as medical devices, motor vehicles subject to type-approval and products certified under the EU aviation safety framework, are excluded if they are already covered by other specific EU sectoral rules. In addition, products intended exclusively for national security and defence purposes fall outside the scope. If your product does not fall into one of these exceptions, the CRA will most likely apply.

Reporting Obligations Applicable from September 2026

While most of the CRA's obligations will not take full effect until December 2027, the reporting obligations concerning actively exploited vulnerabilities and severe incidents impacting on the security of products with digital elements will apply from 11 September 2026. From this date, manufacturers will have a formal legal obligation to report two types of events to the relevant national cybersecurity authorities (CSIRTs) and ENISA (the European Union Agency for Cybersecurity).

Manufacturers must notify actively exploited vulnerabilities, i.e. cases where there is reliable evidence that a malicious actor has exploited a vulnerability in a system without the system owner's permission. This does not cover theoretical risks or known but unexploited flaws; it specifically covers situations where there is reliable evidence that a malicious actor has exploited a vulnerability.

Manufacturers must also notify severe incidents having an impact on the security of their product. These are incidents that negatively affect or are capable of negatively affecting the product's ability to protect the availability, authenticity, integrity, or confidentiality of sensitive or important data or functions or incidents that have led or are capable of leading to the introduction or execution of malicious code in a product or in the network and information systems of a product user.

An early warning notification must be submitted within 24 hours of becoming aware of the vulnerability or incident, and the actual notification within 72 hours. Unless the relevant information has already been provided, a final report concerning the actively exploited vulnerability must be submitted no later than 14 days after a corrective or mitigating measure becomes available, and within one month of submitting the severe incident notification. ENISA is responsible for establishing and maintaining a single reporting platform with national electronic notification endpoints to ensure that sensitive vulnerability information remains confidential.

Crucially, the obligations are not limited to notifying the relevant authorities. Manufacturers are also expected to inform their users of actively exploited vulnerabilities or severe incidents, and, where needed, of the corrective measures that users can take to mitigate the impact of the vulnerability or incident.

But What About AI?

The CRA is not the only significant EU legislation due to take effect in 2026. The general application of the EU AI Act[7] begins on 2 August 2026. A partial postponement of the application timeline has been proposed, particularly with regard to the obligations concerning high-risk AI systems, through the so-called AI Omnibus proposal, meaning that changes to the application timeline may occur in the near future.

The AI Act regulates AI systems and models by setting out requirements and obligations for those who place them on the market, put them into service, or use them in the EU.[8] The AI Act's scope is broad, applying not only to EU-based providers and deployers of AI systems, but also to non-EU providers whose systems are used in the EU, as well as to importers, distributors and manufacturers in the supply chain.

Alongside the CRA, the AI Act brings specific cybersecurity expectations. For 'high-risk AI systems', a category covering AI used in critical applications such as recruitment, credit scoring, biometric identification, and certain critical infrastructure, the AI Act requires an appropriate level of cybersecurity throughout the system's lifecycle. This includes resilience against unauthorised third parties attempting to manipulate the system's use, outputs, or performance by exploiting vulnerabilities.

The good news is that these two regulations are designed to complement each other in relation to cybersecurity requirements. Where a high-risk AI system is also subject to the CRA, compliance with the CRA's essential cybersecurity requirements can be used to demonstrate compliance with the AI Act's requirements in this area. In other words, achieving CRA compliance will also satisfy many of the AI Act's cybersecurity demands.

The AI Act also includes reporting obligations. Providers of high-risk AI systems must report serious incidents to the market surveillance authorities of the Member States in which the incident occurred. In certain situations, deployers of high-risk AI systems must also report serious incidents first to the provider and then to the importer or distributor as well as to the relevant market surveillance authorities. In Finland, market surveillance is the responsibility of the designated supervisory authorities for each sector.

Preparing for Compliance

The obligations set out in the CRA are significant and apply also to the manufacturing stage of products. However, the most pressing task is to establish the internal processes required to detect and report actively exploited vulnerabilities and severe security incidents by 11 September 2026 as mentioned above. Organisations should not consider this as a one-off exercise, but rather as the start of an ongoing compliance programme encompassing, e.g., risk assessments, support period commitments and vulnerability disclosure channels as required by the CRA. For those developing or deploying AI-powered products, the AI Act's application date of August 2026 adds an additional layer of cybersecurity obligations.

Updating Cybersecurity Regulatory Framework Through New Proposals

Digital Omnibus: Harmonising Incident Reporting

The European Commission has proposed a reform of cybersecurity incident reporting obligations, aimed at reducing the reporting burden on businesses. One of the key reform proposals in the broad Digital Omnibus proposal issued in November 2025 is the centralisation of incident reporting under various regulations into a single-entry channel. This channel would be used to submit incident notifications based on multiple different legislative instruments (at least the GDPR[9], NIS2, CER, CRA, DORA and eIDAS[10]) to the competent authorities. The channel would be developed and maintained by (ENISA). This reform would have particular implications for those operators that are subject to multiple overlapping and time-sensitive reporting obligations.

In addition, the **Digital Omnibus proposal would extend the deadline for notifying personal data breaches under the GDPR from the current 72 hours to 96 hours**. The implications of this reform would be broadly relevant to all types of organisations, as all operators act as controllers of personal data in certain situations and are therefore obliged to notify personal data breaches in that capacity.

The Commission's New Cybersecurity Package: CSA2 and Updates to NIS2 Directive

In January 2026, the Commission issued a proposal for a new cybersecurity package to update and supplement the existing core EU cybersecurity legislation.[11]

Through the revised Cybersecurity Act (CSA2)[12], the Commission seeks to address four key challenges: the misalignment between EU cyber policy and stakeholder needs, the failure to implement the European Cybersecurity Certification Framework, the fragmented and complex compliance landscape of cybersecurity regulation, and growing ICT supply chain risks.

- The **ICT supply chain security** proposals are perhaps the most significant reform package within the CSA2, reflecting the impact of the prevailing geopolitical situation on legislation. The CSA2 would create an EU-level framework for managing so-called 'non-technical' supply chain risks. The framework would apply to critical sectors subject to NIS2 regulation and would be based on EU-level risk assessments, on the basis of which the Commission could impose specific requirements and even prohibitions on the use of certain third-country suppliers and their components. If a third country were deemed a country posing cybersecurity concerns, suppliers from those countries would be subject to restrictions relating to, among other things, EU certification, conformity assessment, public procurement and EU funding. For communications networks, the phase-out of high-risk suppliers' components would be based directly on the regulation with corresponding deadlines. Operators with links to countries designated as risk countries could apply for exemptions from the requirements or prohibitions under certain conditions.

- In addition, a key objective of the CSA2 **is to introduce a revised cybersecurity certification framework** that would make cybersecurity certification more predictable, consistent and agile. A key substantive reform would be the expansion of the certification framework's scope to cover ICT products, services, processes and managed security services, as well as organisations' overall cybersecurity posture. This would mean that in the future, organisations could seek certification to demonstrate their cybersecurity level – not just for individual products or services. The role of cybersecurity certification is also intended to be strengthened as a tool for demonstrating compliance and reducing the administrative burden of reconciling obligations under different legislative instruments.

- The CSA2 proposal includes **a comprehensive reform of ENISA's mandate** to enable the agency to support policy implementation and Member States' operational cooperation more effectively. ENISA would be assigned new tasks in supporting operational cooperation, improving situational awareness, operating the EU cybersecurity reserve, and providing reporting platforms and vulnerability management capacity.

In addition to the CSA2 proposal, the Commission's new cybersecurity package includes a separate proposal for amendments to the NIS2 Directive.

The key proposed amendments relate to clarifications of scope, implementing regulations, demonstrating compliance, EU-wide reporting on ransomware, and the supervision of operators providing cross-border services:

- **The scope of NIS2 regulation would be clarified and expanded.** The scope provisions concerning healthcare providers, electricity producers, hydrogen sector companies and chemical industry operators, as well as DNS service providers, would be clarified. Providers of European Digital Identity Wallets and European Business Wallets, as well as operators of submarine data transmission infrastructure, would be brought within the scope of the regulation. A new category of small and medium-sized enterprises would be introduced in accordance with the Commission's recommendation.[13] Small mid-cap companies falling under Annex I of the NIS2 Directive would, as a general rule, be classified as important entities (rather than essential entities), which would reduce the supervisory burden arising from the regulation.

- **The consistency of the regulation's application would be improved through implementing regulation.** The Commission would be required to draw up detailed guidelines on supply chain security requirements to improve the legal certainty and proportionality of the regulation. In addition, further harmonisation would be introduced to specify the requirements concerning cybersecurity risk management measures.

- **Cybersecurity certification would be used to facilitate the demonstration of compliance** (utilising the aforementioned certification framework).

- Under the proposal, **an EU-wide framework for collecting information on ransomware attacks** would be introduced. The objective is to provide authorities with the information necessary to dis-

rupt and dismantle the operations of ransomware groups.

- **ENISA would be given a new role in supporting Member States in the supervision** of operators providing services in multiple Member States. ENISA would carry out a comprehensive analysis of cross-border cybersecurity risks and prepare an annual risk assessment report. On the basis of the report, ENISA could recommend the establishment of joint inspection teams to competent authorities, develop common supervisory guidelines and assist in joint supervisory actions.

- Under the proposal, **Member States would be required to adopt policies for transitioning to post-quantum cryptography (PQC)** as part of their national cybersecurity strategies. The proposed timeline targets a PQC transition by 2030 for critical use cases and by 2035 for medium- and low-level use cases. According to Finland's current Cybersecurity Strategy (2024–2035), one of Finland's strategic objectives is to be self-sufficient in critical encryption technologies and prepared for the quantum threat by the early 2030s.

How to Navigate the Shifting Regulatory Landscape?

While the first wave of cybersecurity regulation earlier this decade was often described as a tsunami, the current situation is better characterised as a regulatory swell. Overall, cybersecurity regulation has been subject to unprecedented turmoil. In some cases, the process of updating the regulatory framework has begun remarkably early, which highlights the importance of actively monitoring developments. The following approaches can support navigation through the evolving regulatory landscape.

Firstly, it is crucial to identify the regulation most relevant to one's own operations, as well as the potential indirect effects of other regulation, for instance through supply chains. Identifying synergies between obligations under different legislative instruments can help to ensure that obligations are implemented in a meaningful way. Rather than monitoring certain regulations and acts, it may be more practical to do so on a category basis (e.g., obligations related to incident detection and handling, supply chain security). For instance, depending on the organisation, the areas of incident and vulnerability management may be subject to multiple, partly overlapping obligations.

The introduction of legislation in the field of cybersecurity risk management has elevated the importance of written cybersecurity documentation to a whole new level. As well as serving as an internal communication and operational tool, documentation is also an important means of demonstrating regulatory compliance for safeguarding legal certainty in the event of incidents, supervisory measures or disputes. As cybersecurity regulation is risk-based, the documentation of risk assessments and risk management measures, as well as keeping such documentation up to date, is a fundamental starting point for risk management work. The regulation encourages organisations to adopt a proactive approach to cybersecurity management.

A clear definition of tasks and responsibilities is essential for the successful implementation of obligations. As risk management becomes increasingly demanding and challenging due to the threat environment and regulation, it is crucial to ensure that teams are adequate and recognise the importance of effective cooperation for sustainable cybersecurity risk management.

AUTHORS:

JOHANNA TUOHINO
Dittmar & Indrenius

JUKKA LÅNG
Dittmar & Indrenius

ROOPE FREDMAN
Dittmar & Indrenius

REFERENCES/SOURCES

1 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

2 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.

3 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements.

4 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities.

5 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

6 Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents.

7 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

8 It should be noted that these requirements are subject to the European Commission's initiative to simplify and partially delay the application date for the obligations set out in the AI Act.

9 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

10 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, amended by Regulation (EU) 2024/1183.

11 Proposal for a Regulation for the EU Cybersecurity Act, COM(2026) 11; Directive Proposal for simplification measures and alignment with the Cybersecurity Act, COM(2026) 13.

12 The CSA2 proposal seeks to revise Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification.

13 Commission Recommendation (EU) 2025/1099 of 11 June 2025 on the definition of micro, small and medium-sized enterprises.

CYBERWATCH FINLAND
& DNV CYBER

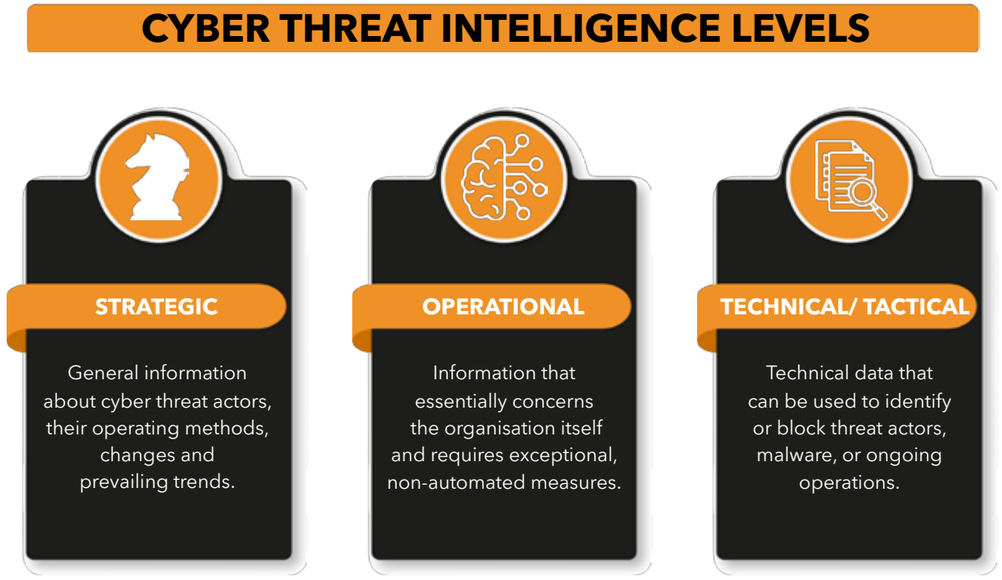
Cyber Threat Intelligence Handbook

Cyberwatch Finland has produced a cyber threat intelligence handbook in collaboration with DNV Cyber, with the aim of increasing the understanding and capability of Finnish critical sector organisations to use cyber threat information. An abridged version has been prepared for this publication. The handbook will be published in spring 2026 in both Finnish and English and will be freely available to all.

Introduction

Cyber threats are constantly changing and evolving, and organisations are increasingly being required to absorb and make use of information concerning cyber threats. This is emphasised not only in current practical needs but also in legislative requirements. Whilst the EU's Network and Information Security Directive NIS2 (EU2022/2555) and its nationally applicable versions (the Cybersecurity Act, the Act on Information Management in Public Administration, and the Act on Electronic Communications Services) do not directly oblige organisations to acquire or make use of cyber threat intelligence, they do require the assessment and management of cyber threats, the development of an organisational cyber risk management model on this basis, and the reporting of significant incidents to the supervisory authority. With the new Cybersecurity Act, company management now bears greater obligations than ever before, and the new requirements place increased emphasis on the personal responsibility of senior personnel for the implementation — and failure to do so — of risk management measures. It is almost impossible to implement cyber risk management measures without real-time threat intelligence, because visibility of the threat landscape then becomes severely limited and unrealistic. The more comprehensive an organisation's cyber threat intelligence is, the more time it has to prepare.

In the modern information society, every organisation must prepare for cyber threats — either directly or indirectly. A cyber threat is a potential situation, event, or action that may damage or disrupt communications networks and information systems, users of such systems, and other actors. Far too often, the level of preparedness within organisations is not sufficient to treat the materialisation of a cyber threat with the seriousness it warrants. Reactive rather than proactive approaches continue to dominate, with measures taken only after a cyber threat has occurred, reputational damage has already been sustained, and the authorities have taken an interest. Meaningful and timely threat intelligence seeks to bring predictability and efficiency to measures taken, whilst minimising the cost of damage. Cyber threat intelligence aims to bring both time and background information to decision-making. For threat intelligence to be of benefit to an organisation, its leadership must also have sufficient capacity to make decisions based upon it in order to steer the organisation in the right direction. Cyber threat intelligence is a prerequisite for increasingly sophisticated and precise data-driven leadership when planning and implementing cyber protection.



Levels of Cyber Threat Intelligence

Cyber threat intelligence refers to information acquired from or relating to the operating environment, concerning which threats are most probable and how to guard against them. In practice, it is information that guides an organisation's decisions regarding cybersecurity investments, operating models, or technical solutions. Cyber threat intelligence, and the process of producing it, closely resembles the intelligence cycle. The traditional intelligence cycle is a continuous, phased model for collecting, analysing, and delivering information to support decision-making. It is important for organisations — and especially senior management — to understand the different types of threat intelligence that are available. Cyber threat intelligence is often divided into three levels to aid comprehension: strategic, operational, and technical (sometimes also tactical) threat intelligence.

Developing and Evaluating the Threat Process

The most important criterion that can be set for threat intelligence is its **actionability**. This means that the threat intelligence an organisation produces or acquires is, by its nature and content, such that it addresses needs, leads to direct action, or confirms the validity of measures already taken. Every organisation has its own resources and objectives, which determine the scope of the threat intelligence process it pursues and the extent to which in-house activity and the use of partners takes place. Growing an organisation's cyber maturity is a process by which it moves from ad hoc security towards a systematic, risk-based, and proactive approach that brings together people, processes, and technology.

The quality of the cyber threat intelligence process can be assessed through cyber maturity. The maturity level indicates the extent of an organisation's cyber capability to protect itself from cyber threats and ensure business continuity in the event of disruption. Cyber maturity grows as working practices and processes are developed in response to feedback and the evolving cyber environment. Measuring one's own maturity level may be necessary when selecting suppliers and other partners. In the case of subcontractors, it is useful to assess their technological capabilities — that is, which systems they use and what data sources they have access to. The cyber threat intelligence process is almost always based on information sharing and collaboration. It is so broad and multifaceted in nature that even the best-resourced organisations would be unwise to attempt to do everything themselves; securing the right partners is an important part of a successful process. Partnerships may take the form of peer-to-peer information-sharing networks or subcontractor and supplier relationships through which information or expertise is acquired. The best partnership is one in which both parties are able to give and receive information, enabling mutual growth and development.

The Cyber Threat Intelligence Process

The cyber threat intelligence process (CTI process) in this handbook is divided into the phases of **direction**, **collection**, **analysis**, and **dissemination**. The aim of the cyber threat intelligence process is to produce additional time for decision-making and to shift from reactive behaviour to a proactive, anticipatory one. Through a cyclical threat intelligence process, it is possible to develop and guide man-

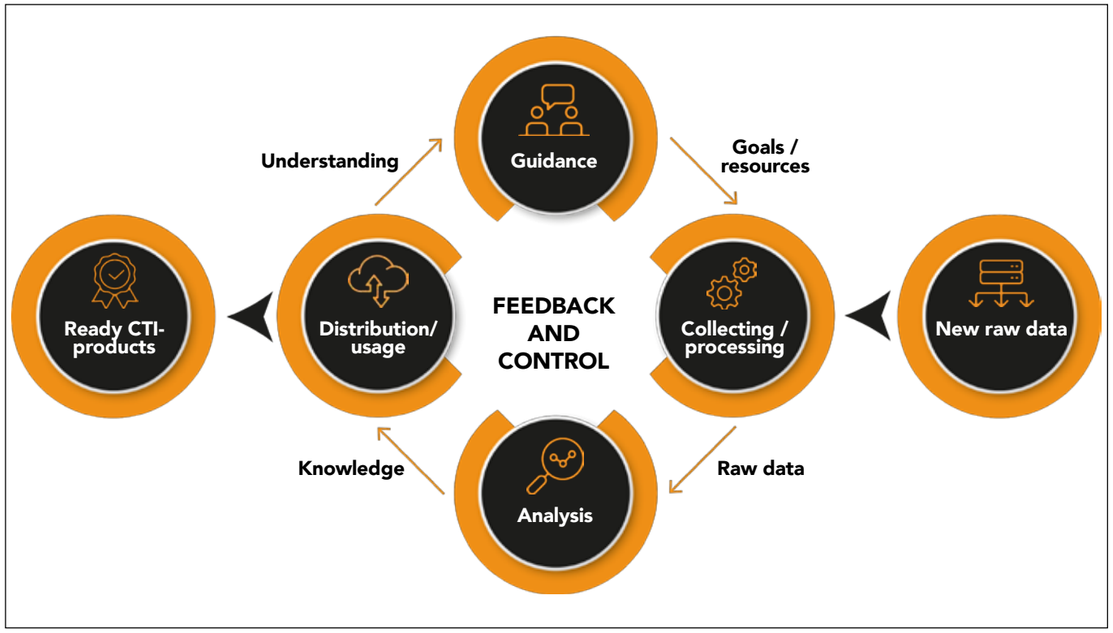


Figure 1: Cyberthreatcircle's singular process

agement's capacity to understand cyber threat intelligence. It encompasses all stages from the initial plan through to the collection and utilisation of information, as well as the implementation of improvements identified during the process in preparation for the next collection cycle. During the process, raw data is shaped into information and ultimately into knowledge that supports or guides decision-making. In practice, each stage of the cycle operates simultaneously alongside the others, and several CTI processes may be running concurrently.

Guidance

The guidance phase of the CTI process is often the most critical for the process's success. In this phase, management defines the process objectives, resources, and mandate for achieving those objectives. Without carefully executed direction, it is likely that resources will be wasted on collecting or processing the wrong type of information, or that not all available and necessary information will be collected or utilised. It is the responsibility of management, through well-executed direction, to protect the organisation's IT assets from various threat actors, as even a single oversight can lead to a significant security incident. In simplified terms, the guidance phase concerns the planning of threat intelligence collection and utilisation, as well as the preparation for the practical implementation of those plans. The CTI process is ultimately a matter of investment in security — such as the protection of IT assets — and if a return on that investment is desired, it ought to be planned and prepared with care.

Collection and Processing

The phase following guidance is collection and processing. Collection refers to the acquisition of information at various stages of processing (whether raw data or pre-analysed intelligence) in accordance with the plans made in the preceding phase. Processing refers to the conversion of collected information into unified, actionable, and contextual threat information for subsequent analysis and use. In other words, in order for information to be utilised, it must first be found and collected. Only once this collected information has been refined does it become usable. When launching a new cyber threat intelligence process, there is a common tendency during the collection phase to gather as much information as possible from as many different sources as possible. Whilst an abundance of information is sometimes beneficial, this approach can easily lead to a situation where there is too much input and security teams become paralysed by spurious alerts and a mass of data requiring manual review. During the collection phase, it is therefore important to bear in mind the needs defined in the preceding phase and to direct activity accordingly. An excess of information can lead to errors just as readily as insufficient collection. Only the most advanced organisations — those with the greatest investment in the cyber threat intelligence process — should attempt to collect all available information.

Analysis

The third phase is analysis. During the analysis phase, the collected raw data is transformed into threat intelligence through the analytical process. Depending on the quality of the data collected, this can be a straightforward exercise or one requiring considerable effort. The aim is to add meaning to the raw data, to combine information from different sources to draw conclusions, and ultimately to produce intelligible information to support decision-making and thus enable concrete action. Of particular importance to the outcome is the clear definition of intelligence requirements and information needs at an early stage of the process. In cyber threat intelligence, analysis may be carried out equally well by a human or a system. Automation and the use of artificial intelligence — particularly in the analysis and processing of technical data — is continually developing, though human analysts continue to play a significant role, especially in strategic-level analysis.

Distribution

The final phase of distribution and utilisation is a prerequisite for the work to be of practical benefit. The most important criterion for what type of threat intelligence an organisation should acquire is its usability. Whether the ultimate recipient of the threat intelligence is a system, an individual, or a department within the organisation, the task of this phase is to ensure that the collected and analysed intelligence reaches its intended destination, and that the recipient knows what they are receiving and what they should do with it. The distribution of cyber threat intelligence concerns both the organisation itself and external partners. The functioning of networks depends on all parties both producing and receiving information; therefore, organisations working with cyber threat intelligence must also be prepared to share the intelligence they have acquired and processed. In particular, there must be complete confidence in the quality of the intelligence being shared, or alternatively, any uncertainty must be expressly communicated. The question to consider is what type of information the organisation is in a position to share and with whom. The criticality of threat intelligence must be determined internally within the organisation, and the various information-sharing networks or partners classified according to what level of information may be shared with whom. The most important task of the distribution and utilisation phase is to ensure that plans are carried out and adjusted as necessary.

Direction of Development

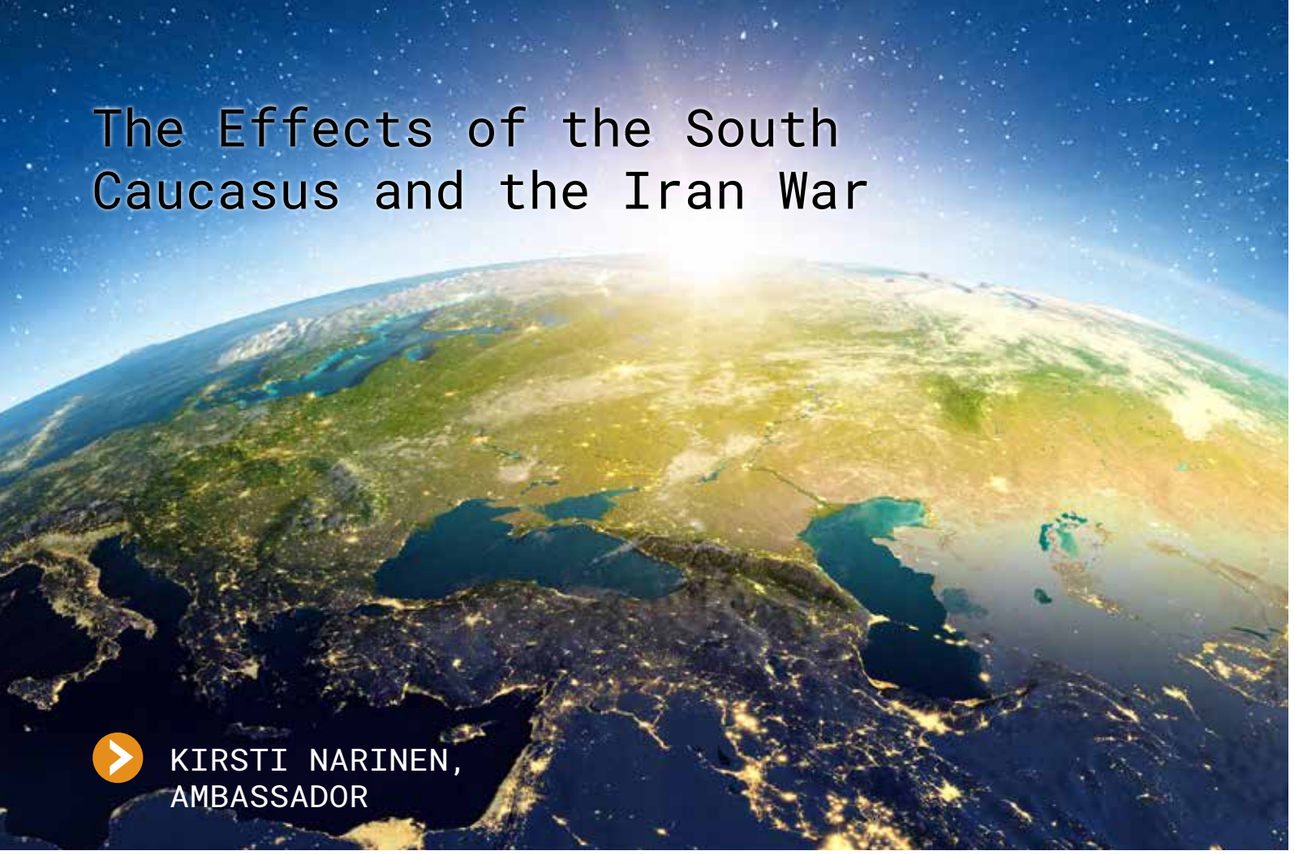
The most important purpose of cyber threat intelligence is to produce time and information for decision-making. The time it provides is intended for the advance identification of and response to threats. This window is continually shrinking, and obtaining early warning is becoming ever more difficult. Threat actors' operations have accelerated, and the time between the disclosure of new vulnerabilities and their exploitation has shortened. At present, one often speaks of minutes between vulnerability disclosure and attempted exploitation. Technological advancement favours attackers, and artificial intelligence, for example, has already provided significant advantages to those carrying out cyberattacks. As a result of the increasingly intensive cyber influence activity, the need for up-to-date cyber threat intelligence has grown further still. The actions needed to protect an organisation's most critical assets are required more rapidly than a human being can implement them. In addition to acute, rapidly actionable intelligence, there is a greater need for strategic and operational intelligence as the overall security situation deteriorates and state-sponsored cyber influence activity becomes more prevalent.

The need for cyber threat intelligence affects every organisation, but not in the same way. The resources and needs available to each organisation determine the individual circumstances in which it operates. The process of acquiring and utilising cyber threat intelligence is quite broad and multifaceted. Successfully implementing it requires motivation, resources, and experience. The cyber threat intelligence process must be understood as a continuously active and evolving function. The cycle must keep turning, and feedback must be gathered on the execution of each phase. The most important factor for the continued development of the process is the willingness to develop it. The cyber threat intelligence process should not be seen merely as an obligatory measure, but as a value-adding investment that may save an organisation from a debilitating incident, financial losses, and reputational harm.

Conclusion

The handbook is primarily intended for Finnish critical sector or defence sector actors falling within the scope of the Cybersecurity Act, though its content can equally be applied more broadly, regardless of an organisation's sector or size. In the handbook, the phases of the CTI process (direction, collection, analysis, and dissemination) are each addressed individually from three distinct perspectives. At the outset of each phase, the handbook covers the responsibilities and actions of organisational management. This is followed by a discussion of operational-level measures and the duties of operational management. Finally, the practical and technical tools available for use at each phase are addressed. The intention is for representatives of each perspective to derive concrete benefit, such that the handbook conveys as comprehensive and cross-cutting an understanding of the entire cyber threat intelligence process as possible.

The Effects of the South Caucasus and the Iran War



KIRSTI NARINEN,
AMBASSADOR

The South Caucasus is a region between the Black Sea and the Caspian Sea — a millennia-old trade route between East and West, once the Silk Road, now the Middle Corridor. For centuries/millennia, it has been the target, victim, partner, or enemy of three regional power centers — Russia, Turkey/the Ottomans, and Iran/Persia — depending on the mutual relations among those three. Of the countries outside the region, Israel has raised its visibility and significance in recent decades, and the USA over the past year. The situation is therefore both new and traditional. Russia's influence in the region is in decline for a number of reasons, and Iran's apparent weakness could offer Turkey an opportunity to seize power — though it does not appear to particularly want this. Russia is a regional power center with which Turkey does not wish to compete in the long run.

The EU's role is increasingly important in particular economically, but its political influence is still searching its format. In spite of its EU candidate status Georgia is sliding down the slopes of democracy further away from the European values. Azerbaijan is first and foremost an energy provider, but its EU relations are developing in some sectors – and Armenia is the only one of the three genuinely expanding its cooperation with the EU.

Azerbaijan

Despite its Muslim identity, Azerbaijan has for years been a close partner of militarily, as well as in the fields of science, culture and technology. In exchange for modern weapons technology, Azerbaijan has provided Israel an important position for regional observation. It is a close partner of Turkey and has also attempted to mediate the tense relations between Israel and Turkey.

With Iran, Azerbaijan has sought to maintain a delicate (positively toned) balance. The relationship has been seemingly stable, but tense. There are ongoing plans to build a new bridge over the Araks border river, there have been presidential-level visits, phone calls, and situation briefings. Efforts have been made to build a south–north trade route with Russian support. Iranian President Pezeshkian is of Azeri ethnicity and speaks Azeri. The Khamenei family also has ethnic Azeri roots.

An estimated 30 million ethnic Azerbaijanis live in Iran. They have no separatist aspirations, and although they primarily live in the north, they have spread throughout the country. A foreign attack has likely strengthened this group's Iranian identity.

On March 5th, Iran fired four drones into Azerbaijan's Nakhchivan exclave, which lies behind Armenia and borders Iran. The attack was a mistake by Iran, who explained it to be an Israeli drone — perhaps one, but not four. Nakhchivan is the ancestral home of Azerbaijani President Aliyev's family, but the area is otherwise politically and economically peripheral. The airport was slightly damaged and flights resumed within a few days. But the political message was clear.

President Aliyev was understandably both furious and concerned. He had stated and felt that he had done everything in his power to maintain neighborly stability. Aliyev ordered the military to full preparedness and demanded an apology from Iran. President Pezeshkian called, expressed regret while denying Iran's involvement. Through his public apology, he announced that Iran would not attack countries from which it had not been attacked. The media interpreted this to be addressed to the Gulf Arab states, but the intention was likely specifically to reassure Baku.

Iran does not need a new enemy in its neighborhood. And president Aliyev has brought his country onto a path of peace with Armenia after decades of hostility — a new open conflict is not needed now. Turkey also likely does not wish to see its partner become a party to war. The interpretation of the drone strike as terrorism remains. The incident is thought to indicate Iran's military use of decentralized decision-making in crisis situations, which in this case the regional chief of command made the wrong choice. President Aliyev responded by prominently arresting Azerbaijani Shia activists. The fear of terrorist attacks is likely not unfounded.

Armenia

Armenians have confidential relations with Iran and connections at many levels, but the relationship is more pragmatic than emotional. For them, Iran is a stabilizing security-political force amid the Turks on either side. The instability caused by a prolonged war would prevent or slow down the peace process between Armenia and Azerbaijan, which took a significant step forward under President Trump's leadership at the Washington summit in August 2025. Connecting the two Azerbaijani regions is a vital part of the peace process and Trump Route for International Peace and Prosperity, TRIPP shall be built but directly on the Iranian border. Proceeding with the project needs to wait till the war ends.

Armenian circles do not consider a change of power in Iran by external forces to be possible. The force for change must be internal, and despite the January riots, they consider the possibility of an anti-theocratic uprising to be small. The system has been built to be resilient. The rise to power of an external figure such as Pahlavi is not likely. He is also opposed by the Azeris — his grandfather, among other things, banned the use of the Azerbaijani language when violently suppressing the Azeri uprising after World War II.

Armenia's relationship with Iran is also economic. There is an energy exchange agreement with Iran covering gas and electricity produced in Armenia, which is of great importance to Armenia's energy security. Twenty-five percent of Armenia's foreign trade passes through Iran. Traded goods arriving from India and China are transferred by truck from the port of Bandar Abbas to Armenia or onward to Georgia and Russia. The closure of the Strait of Hormuz has halted deliveries. During recent years Armenia has found new export markets in the Gulf region — primarily by air, which is now at a standstill. The fear associated with the crisis is therefore primarily economic. Rising fuel prices are increasing inflation and slowing an otherwise well-performing economic growth.

Armenia's multivectoral foreign policy has worked well, and it has no other direct risk of its own except a wave of millions of refugees in an Iranian civil war scenario. Approximately 50,000 Armenians live in Iran — their returning home would also be an economic and social shock, as the country is only just recovering from the forced displacement of Karabakh Armenians (autumn 2023).

Georgia

Georgia's decline in democracy and human rights has accelerated in recent years to a degree that can not anymore in any way be reconciled with its former guiding star of Western orientation and EU candidate status – even if the government continues to ensure that EU memberships is their aim. The Georgian government's vague foreign policy is a puzzle to everyone, likely including themselves. The ruling party Georgian Dream's approach to foreign policy is to sow discord both with enemies and partners, and among them. Iran has not been an exception. Iran has received much more positive attention than even an imaginary Western orientation would allow. The government's post-attack statement on March 2nd managed to include condolences to Iran for the deaths of state leaders and civilian casualties, condolences to Jewish friends and Israel for victims and damage, and on top of those expressions of solidarity with the Gulf region, with which it has good (economic) relations. It concluded with a wish for a swift diplomatic resolution.

Iran's soft influence is well established. A significant number of Iranians live in Georgia as well as the minority group of Azerbaijani-backgrounded Shia activists. Georgia hosts several Iran-linked Shia universities, including the US-sanctioned Al-Mustafa, where in addition to the Quran, anti-Western ideology is taught. Economic hybrid influence is also extensive. Thousands of Iranian-registered companies have been set up recently and are considered mechanisms for circumventing Iran sanctions. Several companies have been found to be close to the government's economic inner circle. Several studies documenting this have prompted the government to summon the researchers for interrogation, accused of treasonous activity. Iran-related revelations do not promise the desired turn for the better in the relations with the United States. The government's value conservatism has not, despite expectations of the ruling party, resonated with President Trump's MAGA politics. Vague patterns of partnership and hostility add no meaningful trust of any kind. Vice president JD Vance visited the neighbourhood in February but excluded Georgia.

Epilogue

Russia views the South Caucasus as its backyard, over which it has a natural right of dominance. Azerbaijan, through its fossil fuel economy and undeniably skillful foreign policy, has a fairly sovereign grip in relation to Russia. Armenia has lost its trust in Russia as a security-political partner, but Russia's economic grip on Armenia is significant. The Armenian parliamentary elections in June are shaping up to be a geopolitical contest between a new multidimensional Western orientation, peace politics, and the old Russian dependency. Russia's hybrid interference – even for the visible part - in the elections is forceful.

Georgia's position is unclear. The country is led from behind the scenes by billionaire Bidzina Ivanishvili, pursuing his own interests more than national well-being. Russia holds Abkhazia and South Ossetia and is a longstanding enemy, even as it appears that the government is accommodating Russian wishes. The power structure operates from its own premises in accordance with Russian interests — for Russia, monitoring is sufficient. Its influence comes straight from the hybrid threats playbook, according to which the main aim of the hybrid influencer is to create a favorable decision making structure. In Georgia the ruling party has done this themselves. The Georgian people appear to understand the situation better than the power structure, keeping the flame of democracy alive under difficult circumstances.

The war has caused and shall cause great concern to the region. Even if the rising price of fossile fuels has brought more money to the Azerbaijani economy while its position as one of the few reliable energy partners for Europe has strengthened, its partnership with Israel is a risk that might lead to unpredictable consequences. The waivering and unforeseeable decision making mechanism of USA and president Trump does not promise the stability to return. If Armenia considers Azerbaijan and Türkiye to be challenging neighbours, from the Azerbaijani angle Iran and Russia are not much different.

Positive for the peace process is that Armenia, Azerbaijan, and Türkiye have easily found common ground over the Iranian crisis. Communication is intensified. All wish for the opening of diplomatic channels and for a swift resolution.

AUTHOR:

KIRSTI NARINEN
Ambassador

Ambassador Kirsti Narinen has been working for the Ministry for Foreign Affairs since 1984, and since autumn 2020 she has served as the Roving Ambassador represented from Helsinki to the South Caucasus; Armenia, Azerbaijan and Georgia. She served in Tallinn as Counsellor in the 1990s and as Ambassador from 2014 to 2018, after which she spent two years as Head of International Relations at the European Centre of Excellence for Countering Hybrid Threats.

Current Legislative Initiatives are Reshaping the Operating Environment of the Cybersecurity Industry

RISTO RAJALA
& PETER SUND

The international security order continues to deteriorate. Already in the first days of the year, the United States launched a targeted military operation against Venezuela, abducted and removed the country's president, Nicolas Maduro. Perhaps emboldened by what it perceived as a successful operation, the US began exerting increased pressure on Denmark and its European partners, demanding the sale of Greenland. This time, however, Europe adopted a firm stance of opposition instead of appeasement and flexibility. International turbulence escalated further when the United States and Israel launched large-scale air strikes against Iran, to which Iran responded by attacking the US, Israel and the Arab countries of the Persian Gulf, as well as threatening shipping through the Strait of Hormuz. Meanwhile, long-standing conflicts such as Russia's war of aggression against Ukraine, the war in Gaza and the civil war in Sudan show no signs of abating. Information and cyber influence operations are being used extensively as tools.

Continuous and accelerating global instability has a strong impact on the digital world, fuelling the growing phenomenon of cyber insecurity – illegal and harmful acts carried out via computer networks. In particular, the war between the United States and Iran may further increase the activity of state-sponsored or state-linked cybercriminals. This may be exacerbated by a possible crisis in the global economy, which could jeopardise the financial capacity of companies and organisations to invest in strengthening their cybersecurity. The US's actions regarding the annexation of Greenland have also amplified calls for Europe to pursue digital sovereignty. Managing the risk to the availability of digital services is a core aspect of cybersecurity. It is hard to overstate how seriously the US's unprecedented political and economic pressure has undermined the trust of its European allies in their key partner.

As geopolitical uncertainty and digital risks increase, the role of the cybersecurity industry as a pil-

lar of societal security is ever more pronounced. Legislation has a significant impact on the operating environment of the cybersecurity industry and, indeed, the entire digital economy and way of life. Well-formulated laws can support the conditions for both the industry and society at large, strengthening digital resilience. Three legislative initiatives are currently of particular relevance: the comprehensive revision of the EU Cybersecurity Act, the national complementary law proposal for the Cyber Resilience Act, and the overall reform of the so-called Evaluation Act, all of which are seen as broadly supporting the advancement of cybersecurity.

The reform of the EU Cybersecurity Act raises hopes

In January 2026, the European Commission introduced legislative proposals for the comprehensive revision of the Cybersecurity Act (CSA2) and amendments to the related NIS2 Directive. The aim of the reform is to create a more effective and unified EU cybersecurity framework by revising the powers of the EU Cybersecurity Agency ENISA, modernising and expanding the certification system for cybersecurity products, and introducing an EU-level mechanism for managing ICT supply chain risks. The proposed revision of the NIS2 Directive ("NIS2.5") seeks to make the directive clearer, easier to comply with and more compatible with the overall EU cybersecurity legislation, while also reducing the administrative burden on businesses.

A key aspect of the legislative proposal is that the regulation brings clarity and predictability to supervision, certification and the management of supply chain risks from non-EU countries. On this basis, the main lines of both legislative proposals are commendable. However, it is vital in further preparation to ensure that the shortcomings of current legislation are addressed.

ENISA, which plays a central role in the reform, and its legal basis must be critically assessed with a focus on the tasks where it can add the most value at the European level – value that member states cannot achieve alone. ENISA currently has too many tasks (estimated at around 170), and it is necessary to significantly reduce this number. Many of ENISA's current responsibilities overlap with other agencies or member state functions, which undermines its ability to achieve its objectives and deliver sufficient results. Any increase in ENISA's operational funding and staff resources must be carefully considered in relation to its legal basis and duties. Changes to ENISA's legal basis should not increase costs for national cybersecurity authorities but should instead result in cost savings – an especially important matter for Finland.

ENISA's current tasks, such as supporting industry and developing best practices, overlap with national authorities and the market. Training, competence activities, public communication and participation in standardisation are more clearly the responsibility of member states and European standardisation bodies. At the same time, ENISA's operational tasks should be emphasised, focusing on countering cyber threats and establishing situational awareness, particularly by supporting the national capabilities of member states. The transfer of responsibilities from member states to ENISA should be based on its ability to deliver more added value or significant savings, without undermining the role of national authorities.

There is a great need for the planned reform of the European cybersecurity certification system. Within the framework of the Cybersecurity Act, not a single product or service certification scheme has been enacted in four years, nor is one expected in the near future. The EU Cybersecurity Agency ENISA has not fulfilled its role in promoting EU competitiveness. The proposed reform of the certification system is a welcome and important step towards clearer, more agile and effective European cybersecurity. Attractiveness should be enhanced by managing certification costs, making certification a useful tool for companies seeking access to the internal market. Demonstrating EU-wide compliance in a harmonised way will facilitate the market entry of products and services and strengthen competitiveness.

The proposal introduces new rules for the security of information and communication technology supply chains, which would represent a significant change from the current situation. The EU could identify critical ICT products and high-risk suppliers from third countries, exclude them from public procurement, EU public support and European standardisation, and ban their use.

The proposed EU-level mechanism for managing ICT supply chain security is necessary. It would be based on a risk-based, technology-neutral approach aimed at identifying critical ICT products (components, systems, devices, services or platforms that are essential to critical infrastructure, key to the functioning of supply chains and whose misuse could cause significant harm) and related supplier dependencies.

Implementation of the Cyber Resilience Act is progressing

Implementation of the Cyber Resilience Act, adopted in 2024, is progressing both in Finland and in the EU as provided for in the transition periods. The regulation creates conditions for the development of software and hardware products designed with security in mind and ensures that products brought to market are fundamentally secure, including those from third countries. The cybersecurity sector has emphasised that the objectives of the regulation will not be achieved without effective implementation in EU Member States. The government's proposal for legislation to implement the Cyber Resilience Act partially addresses this need and is currently under consideration by Parliament.

The national implementation law is laudable in many respects. It makes sense to concentrate the market surveillance authority's tasks for the Cyber Resilience Act in the Finnish Transport and Communications Agency (Traficom), due to the agency's expertise and synergies. Finland should also seek to ensure at EU level that there are no significant differences between Member States in the application and market surveillance of the regulation. The aim must be to ensure that Finnish businesses are on an equal footing with those in other Member States in terms of the application of the Cyber Resilience Act.

With the increase in supervisory and official tasks, it is important to ensure operational efficiency. Attention should be paid to vulnerability management and the conditions for receiving mandatory vulnerability reports, as the law already imposes very tight time and quality requirements on reporters. If necessary, other tasks such as the investigation of security breaches and technical advice should be transferred more extensively to market operators through appropriate cooperation arrangements.

A key element of the law is the organisation of the operations of notified bodies assessing the conformity of products and software. These assessment bodies will have a significant impact not only on the operating environment of the cybersecurity industry, but also on the competitiveness of Finland's main export sectors. The draft law proposes to designate Traficom as the authority responsible for notifications under the Cyber Resilience Act, making it the principal organiser of national assessment activities.

Successful national implementation of the Cyber Resilience Act creates competitive advantages and economic growth for companies operating in Finland, which in turn supports the balancing of public finances. Notified bodies will be particularly beneficial for export companies in Finland, as they will be able to bring products subject to the regulation to the EU internal market more reliably and quickly than their international competitors. It should be noted that, for example, in 2025, the value of Finland's CRA-linked goods exports (electronics, ICT products and machinery and equipment) was around €27.3 billion, accounting for about 37% of the country's total goods exports. For this reason alone, conformity assessment must not become a bottleneck

for the market entry of domestic products. In addition, bodies operating in Finland make it possible to offer services to device and software manufacturers and importers operating throughout the EU as service exports. The Cyber Resilience Act also enables the establishment of test environments facilitated by public authorities, for example for testing different products or conditions. A similar procedure is also included in the EU AI Act.

The reform of the National Evaluation Act strengthens the credibility of evaluation activities

The government is currently preparing amendments to legislation governing the security and preparedness evaluation of public authorities' information systems and communications arrangements. This is a comprehensive reform of evaluation legislation, which strengthens the crisis resilience of public administration, clarifies the responsibilities of authorities and improves the availability of security assessments for information systems. The cybersecurity sector has sought to promote the clarity of evaluation procedures, close cooperation between evaluation authorities and the efficient use of private entities in evaluation work.

A central aspect of the reform of the Evaluation Act is that preparedness evaluation is incorporated into the law, which strengthens the ability of authorities to ensure the continuity of operations during disruptions and emergencies and supports the objectives of the Information Management Act. In addition, the evaluation and approval of security-critical solutions and their manufacturers in legislation increases transparency, harmonises procedures with EU and NATO requirements, and improves the competitiveness of domestic actors. The proposed role of the Defence Forces as an evaluation authority responds to growing needs, but its definition and resource allocation should be carefully planned to ensure it does not restrict the activities of private evaluation bodies or cause unsustainable costs for public finances.

The proposed obligation for government authorities to assess their own activities and risks, covering both self-assessment and independent assessment in certain security classes, improves risk management and clarifies the division of responsibilities. Expanding and specifying evaluation procedures, including evaluation by a service provider on behalf of the authority, increases the availability of evaluations and supports business conditions. Updating evaluation criteria ensures that they reflect technological development and cybersecurity requirements, strengthening the consistency and relevance of operations.

Making the approval procedures for the qualifications of evaluation bodies more flexible promotes market efficiency, and the use of corporate security clearance increases reliability. Strengthening cooperation and information exchange between evaluation authorities and the possibility to use private entities to support evaluations improves efficiency and harmonises interpretations, while supporting the development of business.

Active advocacy work to improve the operating environment continues

If successful, the revised Cybersecurity Act, the implementation law for the Cyber Resilience Act and the comprehensive reform of the Evaluation Act will be a significant step towards a better digital life and economic growth enabled by new business opportunities. Finnish Information Security Cluster has been strongly involved in all three legislative initiatives at various stages of their preparation, promoting cooperation between the private and public sectors and building trust.

AUTHORS:

PETER SUND
CEO
Finnish Information Security Cluster (FISC)
Technology Industries of Finland

Jukka Rapo

RISTO RAJALA
Advisor
Finnish Information Security Cluster (FISC)
Technology Industries of Finland

Cyberwatch Finland
WEEKLY REVIEW
9/2026

Theme Review
UKRAINA

Cybersecurity is Built by Small Actions and Management of Large Concepts

Cyberwatch Finland

WEEKLY REVIEW

9/2026

- The focus of Russian cyber operations in Ukraine has been on intelligence gathering. The more prominent cyberattacks have mostly been committed against countries supporting Ukraine.

- Ukraine has emphasised the importance of offensive cyber operations and last summer we got an example of what they look like, as Aeroflot suffered significant losses due to a cyberattack. Russia has tried to defend against Ukrainian operations by moving towards a state-controlled digital ecosystem.

- The number of cyberattack utilising artificial intelligence has increased exponentially during the fourth year of the full-scale war, and nowadays an attack that does not incorporate AI at all is a rare curiosity.

Another year has gone by, and we now enter the fifth year of the full-scale war in Ukraine. In order to commemorate the anniversary and the Ukrainian efforts to repel the attack, Cyberwatch Finland once again publishes a themed review about the cyber events of the past year of the conflict. The fourth year of the war was characterised by the rapid increase in the use of artificial intelligence in cyberattacks. During the Kyiv International Cyber Resilience Forum 2026, a Ukrainian spokesperson stated that around 90% of Russian cyberattacks are in some way currently employing AI. This reflects the wider global trend of growing AI usage in all aspects of life, and it has therefore been a hot topic in cybersecurity as well.

An interesting point that was raised during the forum in February was the increased targeting of the private sector. In Ukraine, more than 50% of all cyberattacks target private corporations, and a similar pattern can be recognised on the other side of the frontline as well. It makes sense: private corporations are often easier targets due to more relaxed cybersecurity practices. This is why the Ukrainians label faster adaptation to rapidly developing threats their greatest challenge at the moment. Ordinary non-military citizens need to be trained to understand how to protect themselves and their workplaces from advanced cyber threats. Technological solutions exist, but the training of personnel just cannot keep up.

One interesting way to solve this issue is the brand-new initiative to entice more women to choose cybersecurity for their studies. Part of the problem is the fact that most IT professionals are male, and thus a significant proportion of them are either currently serving on the frontline or at the risk of being ordered there in the near future. As the Head of the Information and Cyber Security Directorate at the Office of the National Security and Defence Council of Ukraine Nataliya Tkachuk said, getting more women into cybersecurity is not a question of gender equality; it is a question of survival.

Head of Ukraine's State Service of Special Communications and Information Protection Oleksandr Potii said during the forum that Russian cyberattacks towards Ukraine's critical infrastructure are increasingly focused on intelligence gathering rather than disruption of systems. This includes the energy sector, which has been under heavy pressure throughout the war but especially so this winter. Russia is using cyber to gather information about the locations of critical facilities and then targeting them with missile and drone strikes. Presence in Ukrainian systems is then used to assess the effectiveness of the strikes and the repair efforts of Ukrainians. This is an excellent example of how Russia is using cyber as a support element for kinetic operations, a trend that has been growing throughout the year. As Potii said: "Cyberattacks on critical infrastructure never happen on their own; they are always part of a broader operation."

The reasons for the shift towards less disruption and more intelligence gathering are twofold. First, Russia seems to have understood that the war is going to take a long time, and as such the value of intelligence has increased. It will allow Russians to better plan operations in the future, since a quick victory is unattainable. Second, causing damage to systems is much more efficient through kinetic means than with cyberattacks, since Ukraine has been very successful at defending against severe cyber threats. Russia is now trying to optimise its use of resources by choosing the best tool for the job, rather than trying everything and hoping something works.

Russia obviously remains the greatest cyber threat to Ukraine, but it is not the only one. In addition to Russia-linked operations, activity is also recorded from Belarus, China, and North Korea. This hardly comes as a surprise, since these countries are often seen working together. North Korea has gone so far as to send troops to fight alongside Russia, and reports of tightening cooperation between the two countries in the cyber domain have been floating around for a while. Belarus is very likely in a similar position, since they have been extensively helping Russia since the beginning of the full-scale invasion, which partly originated from the Ukraine-Belarus border. China, however, is a different case. It is very much possible that they are not coordinating actions with Russia but rather have their own individual operations going on in Ukraine. China has traditionally been very hesitant to work together in cyber operations, so changing course right now would be rather surprising.

The trend of moving from disruptive attacks towards espionage is true for other targets besides critical infrastructure as well, since it has proven to be the most successful strategy for Russia during the past year. Russian disruptive cyberattacks have largely been focused on countries supporting Ukraine, since achieving disruptive or destructive objectives with kinetic operations is not an option the way it is for targets within Ukraine. Examples of such attacks include the control system breach of a hydroelectric dam at Lake Risevatnet in Norway in last April and the more recent attack against the Polish electrical grid at the end of December. Characteristic of both attacks was the fact that they targeted electricity production, which Russia has been targeting in Ukraine as well, albeit through kinetic means. Inside Ukraine the most notable disruptive attacks targeted the country's railway systems in March and the grain industry during the summer.

Ukraine has not been resting on its laurels either and last summer we were able to read about a major cyberattack against Aeroflot, Russia's national aviation company. To many people, it definitely came as a shock, since the hackers were able to penetrate all of the company's systems. The price tag rose to tens of millions of dollars, but perhaps even more significant were the reveals regarding the company's leadership and the amount of displeasure Russian passengers felt when their flights were cancelled in the middle of the holiday season. For the Russian authorities, the incident was extremely embarrassing, and their attempts to downplay the effects of the attack were largely unsuccessful.

The Ukrainian government has not officially admitted to being behind the attack, but the groups responsible for it are known to have strong ties to the country. What Ukrainian officials have publicly said is very limited for reasons limited to operational security: offensive cyber operations are an important part of their toolkit, but they refuse to comment on any details. The role of offensive operations has been increasingly emphasised throughout the war, and it seems we are finally starting to see tangible results reported by media as well. It seems extremely likely that the fifth year of the full-scale war will include even more cyberattacks against Russia, and some might even argue that Ukraine is consolidating its position as the dominant side in the cyberwar.

Changes in Russia

Meanwhile, Russia has been trying to crack down on commercial messaging apps and to push people to use the government-controlled Max instead. On the list of services now available only through the use of a VPN are ones such as WhatsApp, YouTube and Discord. Even Telegram, one of the most popular messaging services in Russia, is being targeted, despite the pushback from citizens and some officials alike. Near the Ukrainian border, Telegram is often used for emergency updates, and some military personnel even use it for coordinating logistics. It is quite clear that Russia is aggressively moving towards a state-controlled digital ecosystem similar to China, which lets the government monitor and control the content that is being consumed by the public.

There have also been broader restrictions on mobile networks in general, supposedly to counter Ukrainian drones. In addition, authorities introduced a 24-hour mobile internet blackout for anyone entering the country with a foreign SIM card in October, which has sparked significant criticism from people who frequently cross the border for business purposes. The disruptions on mobile network availability are naturally more severe near the Ukrainian border. The Russian military has been employing Starlink to facilitate communications in the area, but SpaceX took action to stop that from happening at the beginning of February. Together with the restrictions on Telegram-use, the loss of Starlink connections has severely impacted Russian military communications, and there are no comparable alternatives available. Russia will face difficulties particularly regarding the speed of communications, coordination of mobile groups, and transmission of drone feeds.

One surprising consequence of the war has been the withering away of Russia's illegal data market, the so-called probiv (пробив). Due to corruption, Russia has been the promised land of data and information leaks, where data from both commercial and official information systems has been sold on the dark web. This information has been used by opposition activists and investigative journalists, among others. One of the most popular categories of information has been the so-called "mobile probiv", which consists of information related to the desired phone number, such as phone and message logs. Other commonly sold information has included people's passport information, access to the FSB border crossing database, and airline passenger lists.

It is believed that probiv contributed to the successes of Ukrainian intelligence, such as the assassinations of high-ranking commanders of the Russian army. This has led to Russia starting to take a harsher approach to information leaks than before. In 2024, the legislation was reformed, and the illegal use, transfer, collection or storage of data is now punishable by up to 10 years in prison. Examples of arrests have also been seen. In the summer of 2025, seven employees of the Interior Ministry's data centre were arrested in Moscow on suspicion of abuse. Tougher penalties and arrests have led to operators leaving the illegal data market, and the prices of the remaining data packages have risen significantly.

All in all, the fourth year of the cyberwar has been marked by the use of artificial intelligence, the shift in the focus of Russian cyber operations towards intelligence gathering, and the increase in Ukrainian offensive cyber operations. At the same time, Russia has tried to counter Ukrainian operations, for example, by moving towards a state-controlled digital ecosystem similar to China. At the beginning of the large-scale attack in 2022, there was a lot of thought about the role of cyberattacks in the war. In worst-case scenarios, the possibility of some kind of "cyber apocalypse" was even discussed, in which a significant part of the functions of modern society would be paralysed by cyber means. So far, we have not seen anything like this, but the understanding of the significance of cyberattacks in the context of war has certainly become clearer. The fifth year of the war is likely to include more Ukrainian cyberattacks while Russia focuses on hybrid warfare against countries supporting Ukraine and intelligence gathering on Ukrainian systems.

Significant Cyber-attacks of the Fourth Year of the War

UKRZALIZNYTSIA

DATE: 23.3.2025
DESCRIPTION: In March 2025, the Ukrainian state railway company experienced a serious cyberattack with the aim of stopping train traffic. The railway network plays a key role in transporting not only civilians, but also soldiers, the wounded and military material.
THREAT ACTOR: The attack has not been attributed to a specific hacker group or security service. However, it seems clear that Russia was behind the attack.
IMPACT: The attacker used malware to suspend the operation of a railway company's website and mobile application for several days. The problems began on the 23rd of March, and some services were still out of operation even at the beginning of April, even though 90 per cent of the services were reportedly restored. In practice, the malware prevented train passengers from buying tickets on the railway company's website and mobile application, in addition to which it affected the operation of freight dispatchers' online services. The technical details of the attack are unclear, but the attack caused long queues and disrupted the rail services.

AEROFLOT

DATE: 28.7.2025
DESCRIPTION: Perhaps the most visible event of the cyber war between Ukraine and Russia was seen in July, when the attackers, who had been preparing an attack on Aeroflot's systems for more than a year, carried out their operations. As a result of lengthy preparations, they had gained administrative access to all of the company's systems. The attackers were able to steal practically all of the company's data. In addition, they destroyed a huge number of the company's systems.
THREAT ACTOR: The pro-Ukrainian hacker groups Silent Crow and the Belarusian Cyberpartisans carried out the attack in cooperation.
IMPACT: During the first day, 108 flights were cancelled and there were more than 80 delays at Sheremetyevo Airport alone. If Aeroflot had not immediately cut off its connections to all possible services and eventually also to its headquarters, its IT systems would have been completely destroyed. However, Aeroflot managed to return to normal operations in just a few days, but the stolen data will torment the company for a long time to come. What was particularly embarrassing was that the attackers published evidence of the company's cooperation with the Russian armed forces, even though Aeroflot has repeatedly publicly denied any involvement in military activities.

ELECTRICITY GRID IN POLAND

DATE: 29.12.2025
DESCRIPTION: The Polish electricity grid was targeted by coordinated cyberattacks at the end of the year 2025. The event is a prime example of Russia's hybrid operations on countries supporting Ukraine. Russian hackers have also attacked critical infrastructure in Norway, for example.
AUTHOR: The attack is attributed to the Sandworm hacker group of the Russian military intelligence GRU. Sandworm was also behind the 2015 and 2016 attacks on Ukraine's energy infrastructure.
IMPACT: The attack affected the communication and control systems of Combined Heat and Power (CHP) plants, as well as the systems that manage the distribution of renewable energy systems from wind and solar power plants. The attack did not lead to any power outages, which may have given a false impression of a weak or unsuccessful attack. In fact, many of the systems were damaged beyond repair. The attack is estimated to be the largest Russian sabotage attack on Europe so far.

SOURCES:

https://carnegieendowment.org/russia-eurasia/politika/2026/02/russia-starlink-telegram-shutdown

https://www.dragos.com/blog/poland-power-grid-attack-electrum-targets-distributed-energy-2025

https://therecord.media/ukraine-cyberattacks-guiding-russian-missile-strikes

https://euromaidanpress.com/2026/01/27/security-service-of-ukraine-blocked-14000-russian-attacks-since-2022/?utm_source=chatgpt.com

https://regard-est.com/ukraine-facing-the-intensification-of-russian-cyber-attacks

https://industrialcyber.co/critical-infrastructure/russian-linked-uac-0219-group-escalates-attacks-on-ukraine-government-critical-infrastructure/#:~:text=CERT%2DUA%2C%20which%20named%20the,agency%20planned%20to%20cut%20salaries.

https://www.reuters.com/world/europe/ukraines-railways-restore-half-it-services-hit-by-cyber-attack-so-far-2025-04-09/

https://therecord.media/russia-sandworm-grain-wipers

https://meduza.io/en/feature/2025/07/29/too-much-is-slipping-through

https://zona.media/news/2025/07/13/probiv

https://www.theguardian.com/world/2025/dec/26/russia-selling-personal-data-leaks-probiv-ukraine-spies

https://therecord.media/whatsapp-russia-blocked-state

https://therecord.media/russia-throttles-telegram-pushes-its-own-messaging-app

Cyberwatch WEEKLY

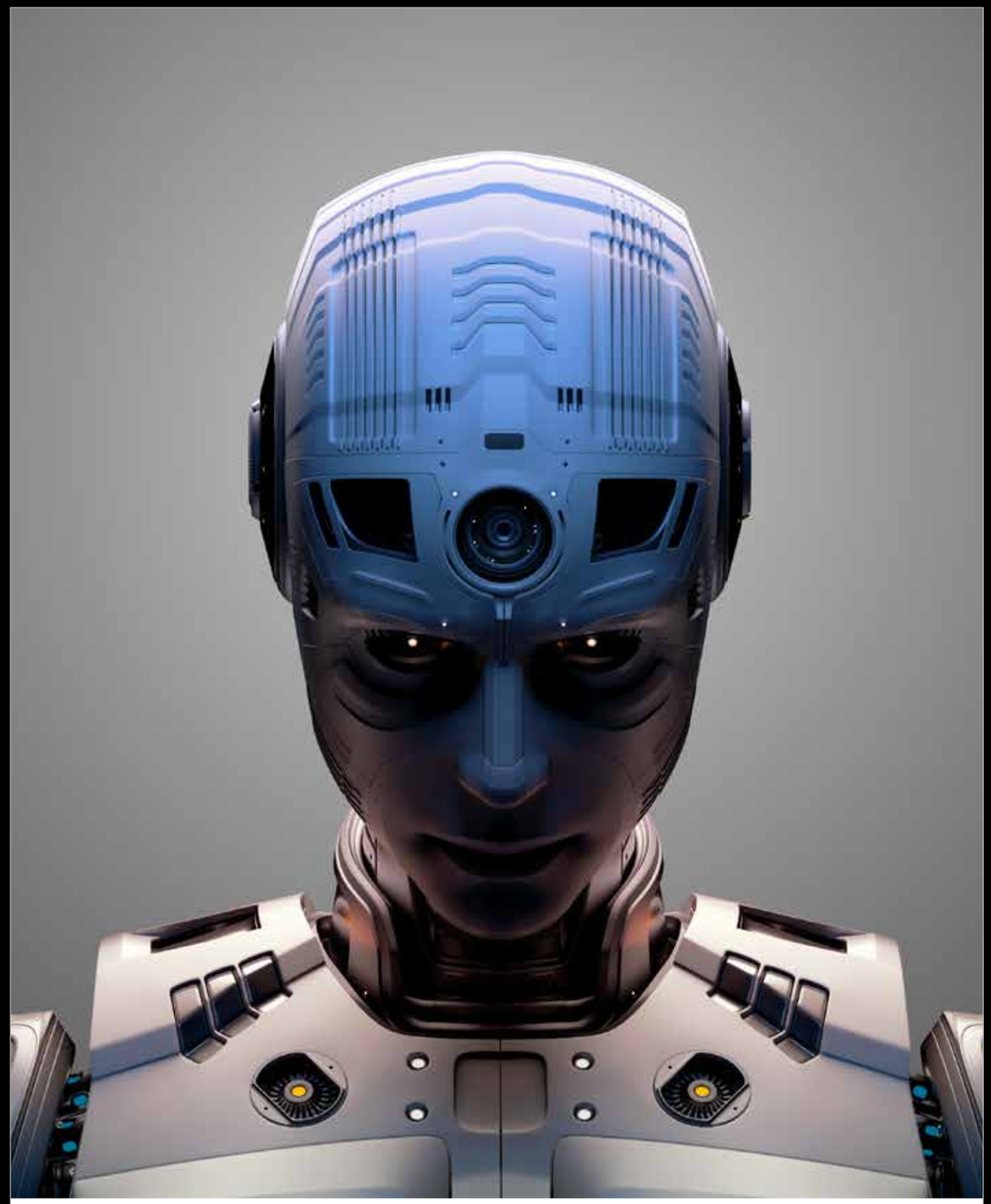
PUBLISHER Cyberwatch Finland | Nuijamiestentie 5 C, 04400 Helsinki | www.cyberwatchfinland.fi

Cyberwatch Finland

MONTHLY REVIEW

APRIL/2026

Cybersecurity is Built by Small Actions and Management of Large Concepts



In this Review

In this monthly review, we examine the most significant cyber phenomena of the previous month and tie them into larger concepts. The review is divided into three perspectives: the most significant events in the cyber world during the month, phenomena that we want to highlight in particular, and those whose development is worth monitoring.

1 EVENTS IN THE CYBER LANDSCAPE

March once again demonstrated how cyber threats and geopolitical conflicts are becoming increasingly intertwined. Iranian cyber operations were highly visible, with attacks targeting not only American and Israeli targets but also a wide range of other countries, especially in the Middle East. The Dutch intelligence services warned in March of a Russian cyber espionage campaign aimed at hijacking the Signal and WhatsApp accounts of journalists, government officials, and military personnel. In the Baltic states, Russia has been accused of running a deliberate online disinformation campaign claiming that the countries were allowing their airspace to be used for Ukrainian drone attacks. The EU, in turn, added two Chinese and one Iranian company to its sanctions list due to cyberattacks carried out against EU member states.

Among the month's concrete cyberattacks, American medical device manufacturer Stryker fell victim to a cyberattack that disrupted Microsoft-based systems and had knock-on effects on both production and supply chains. The attack was linked to the Iran-affiliated group Handala Hack Team. Independent cybercriminals and hackers have also been active. Elixia, a popular gym chain in Finland, suffered a data breach in which customers' names and contact details, among other information, were compromised. Globally, according to statistics from cybersecurity firm Cyber Intelligence House, ransomware groups listed over 2,000 new victims on their sites in March alone.

On the technical sphere, a critical vulnerability discovered in March in the popular software company Citrix's NetScaler ADC and NetScaler Gateway products (CVE-2026-3055, CVSS 9.3) became the target of active exploitation. The incident further highlights the accelerating cycle of vulnerability exploitation: the time between the disclosure of a vulnerability and its active exploitation is constantly shrinking.

The risks of AI technology were also prominent. Internet giant Meta experienced internal chaos when an AI agent published content on an internal forum without user approval due to excessive access rights. As a result, sensitive information was exposed to unauthorized individuals for approximately two hours. A vulnerability was discovered and patched in OpenAI's ChatGPT that would have allowed users' conversation data to be stolen via a malicious prompt. Luckily it was reportedly not exploited in any cyberattacks before being fixed.

Preparing for geopolitical risks requires active situational awareness as well as careful protection and regular updates of devices and software. As the Citrix case demonstrates, attackers are quite agile and quick to exploit known vulnerabilities. As AI becomes more widespread, its use and governance may become a matter of life and death for organisations. To reap the benefits, training on AI-related cyber risks should be rolled out in every organisation, and access rights to AI systems should be strictly limited in order to avoid embarrassing data leaks.

2 IN THE SPOTLIGHT

2.1 Key Personnel are not Immune to Russian Phishing

A broad and coordinated campaign by Russian state-linked hackers to compromise Signal and WhatsApp accounts has drawn warnings from intelligence agencies on both sides of the Atlantic. The Netherlands' Defence Intelligence and Security Service (MIVD) and General Intelligence and Security Service (AIVD) confirmed that Dutch government employees have been targeted, with the operation relying on phishing and social-engineering techniques that abuse legitimate authentication features to covertly monitor messages.

The FBI later issued a public service announcement — the first to directly attribute these campaigns to Russian intelligence services — warning that the attacks are designed to bypass end-to-end encryption not by breaking it, but through account hijacking. The campaign targets individuals of high intelligence value, including current and former government officials, military personnel, political figures, and journalists, and has already resulted in unauthorised access to thousands of accounts globally. These warnings were echoed by French authorities as well.

Attackers employ two primary methods. The first involves abusing "linked device" features: attackers impersonate a trusted contact and send a malicious link or QR code, and if the victim interacts with it, the attacker can link their own device to the victim's account, gaining ongoing access without immediately locking the user out. This method was already employed by Russians to target Ukrainian Signal users a year ago, but now it is being used against other countries as well. This shows the importance of following the developments of the war in Ukraine, since it can allow organisations to prepare for new threats like this in advance.

The second method is a full account takeover, in which victims receive messages posing as official support notifications and are urged to share verification codes or two-factor authentication credentials. A particularly deceptive aspect of the takeover method is that victims can re-register their phone number and regain access to their locally stored chat history, potentially leading them to assume nothing is wrong — an assumption Dutch authorities stress could be incorrect. It is easy to see how thousands of people could have already failed to identify the phishing attempts as such, but at the same time the sheer volume of victims is very worrying, especially given the nature of the targets as individuals with access to classified or otherwise highly valuable information. It remains to be seen how the Russians plan to exploit the fruits of their highly successful phishing campaign, but organisations that fell victim to these attempts should remain alert for any follow-up operations.

Dutch military intelligence chief Vice-Admiral Peter Reesink underscored a broader lesson for everyone: despite their end-to-end encryption, messaging apps like Signal and WhatsApp should not be used as channels for classified or sensitive information. That said, the services themselves remain secure. Once again, the incident was only made possible through human error in failing to recognise the messages as phishing. Authorities across the Netherlands, France, and the United States are advising users never to share verification codes, to regularly audit linked devices, and to treat unexpected support messages with suspicion. Since Russian intelligence operations in Europe have become much more difficult after the start of the war, the significance of cyber intelligence and stolen accounts will most likely increase even more in the future.

2.2 Cybersecurity-based US Router Ban will Lead to Weaker Cybersecurity

On March 23, 2026, the US Federal Communications Commission (FCC) added all consumer-grade routers manufactured outside the United States to its "Covered List," effectively banning the import of new foreign-made consumer router models, citing cybersecurity risks. The decision followed a determination by a White House-convened interagency panel that foreign-produced routers introduce supply chain vulnerabilities and pose severe cybersecurity risks that could disrupt U.S. infrastructure, enable espionage, and facilitate intellectual property theft.

The move was prompted in part by a series of cyberattacks attributed to Chinese state-linked hacking groups. The FCC specifically referenced the Volt, Salt, and Flax Typhoon campaigns, which exploited router vulnerabilities to target vital U.S. infrastructure. China is estimated to control roughly 60% of the U.S. home router market, making this a particularly sweeping action. Notably, the ban applies regardless of the brand's nationality — American companies like Netgear and Amazon-owned Eero are not exempt, since their products are manufactured overseas. Nearly all routers currently on the market are produced outside the U.S., primarily in China, Indonesia, Taiwan, Thailand, or Vietnam, meaning this amounts to a near-total ban on new router models.

There are important caveats: consumers can continue using previously purchased routers, and retailers can still sell models that already received FCC authorisation. Manufacturers can also apply for "Conditional Approval" exemptions from the Department of War or Homeland Security. Critics have raised concerns about practical consequences. Analysts warn that router supplies could tighten and prices may rise. Some commentators have characterised the ban as the government overstepping into consumer choice, given how few routers are actually made domestically. The ban's long-term effectiveness will likely depend on how the conditional approval process plays out.

If approvals are rarely given, the ban will likely result in American retailers running out of newer router models quickly despite price hikes. In the long term, US consumers could then be forced to keep using older router models with weaker security than newer ones – the direct opposite of what the intention of the ban is. It is also noteworthy that since the ban does not differentiate between countries, European companies are essentially regarded as untrustworthy as well. This could be seen as yet another fracture in transatlantic relations. It also means that China is going to be looking for an alternative market for its new router models, and Europe is a likely candidate. With ongoing talks about the security of Chinese devices in Europe, the EU will soon face a hard decision of whether to allow an increasing flow of Chinese technology into the Union or not.

In that sense, the US decision fits quite well to a larger global trend of digital sovereignty. Other examples of this include the Chinese ban on the products of Western cybersecurity companies and the Russian move towards a China-like authoritarian digital ecosystem. Both were based on "security concerns", but at least in the case of Russia, the real goal is for the government to have a stronger grip on the digital communication of Russian citizens.

While cybersecurity concerns in the case of the US are certainly valid, it seems likely that supply chain vulnerabilities were seen as a much more severe problem when designing the ban. The US are clearly trying to encourage more routers to be built domestically to not face catastrophic consequences if China decides to stop shipments to the US in the future. Europe should probably take such risks into consideration as well. That said, going the American route of banning all new router models would inevitably lead to weaker cybersecurity in the short term, so looking for alternative options is important.

3 FOLLOW THESE

3.1 Claude's Ability to Understand Old Programming Languages is a Security Threat

Anthropic's flagship AI Claude has recently mostly been in the news for the company's stance on not allowing its use in automated weapon systems. From a cybersecurity point of view, however, the model's feature that aims to make updating ancient legacy code easier is much more interesting. There are still quite a few examples of systems that are based on code from the 70's, and in many cases, they use a programming language that virtually no one understands anymore. Claude attempts to solve this problem by providing a tool that is fluent in languages like COBOL and can thus help programmers update their systems to more modern ones.

Claude can essentially take care of the most tedious and time-consuming part of the modernisation process by mapping the entire system and its dependencies while documenting the process in a way that is easier to understand for modern programmers. It can automatically detect and flag vulnerabilities to draw attention to the most important problems with the code. This all sounds like fantastic news for cybersecurity, until one realises that the same capabilities are also available for any and all threat actors. Automatic detection and flagging of vulnerabilities do not sound as good when they are being used for attacking a system instead of fixing it.

To make matters worse, many of the aforementioned ancient programming languages like COBOL have actually partially relied on their obscurity for security purposes. After all, if threat actors cannot understand the language a system uses, they are much less likely to discover any vulnerabilities within it that could be exploited. AI is now changing this. If organisations that still rely on legacy code do not act soon, criminals and other bad actors certainly will. Obscurity is no longer a form of protection the way it used to be, so modernising legacy code has become much more urgent a task than before.

There are many such systems in Finland as well, and quite often they are found in systems related to critical infrastructure. Until all of them are thoroughly updated, any adversaries that want to attack them have a significant advantage thanks to Claude. There are of course systems in place to prevent people from using the model for nefarious purposes, but as the model itself put it when asked about threat actors using it for attacks on COBOL-based systems: "Yes, honestly — in that specific scenario, my knowledge could be a meaningful enabler."

It is good to remember that the model still does not work as an automatic attack tool. It can only help an attacker understand code written in a language they do not know or analyse it for vulnerabilities. In many cases, however, that could be the deciding factor that enables an attack. Perhaps the most significant threats in this case are insider risks. An unsatisfied or angry employee with basic programming knowledge could cause some serious problems with the help of Claude if they really wanted, since they might have easier access to the code that Claude could then help analyse. With the amount of easy-to-use ransomware-as-a-service tools available, it would take very little effort for someone to engineer an effective attack from the inside.

Although Anthropic has been framing this capability as a boost to cybersecurity, it could turn out to be the opposite, at least in the short term, while systems are not yet updated. A cynical way to think of it is this: Anthropic does not need to care whether it is the organisations trying to modernise their systems or the threat actors trying to attack them that use Claude to search for vulnerabilities in legacy code, for they make money all the same. As with everything else, AI seems to be rapidly accelerating the pace of development here as well. Unfortunately, it is probably just a matter of time before we see news of Claude being part of an attack on a COBOL-based system that would not have been possible before.

3.2 Demand for Stolen AI Accounts Increases Criminals' Interest in Credential Theft

Researchers recently published findings suggesting that premium AI-account credentials are becoming an increasingly desired commodity for both sellers and buyers on dark web marketplaces. Last year, cybercriminals were selling roughly 400 stolen generative AI account credentials per day on underground Russian-language marketplaces, with many of those credentials harvested from corporate users' machines infected with infostealer malware. In one notable incident, over 100,000 ChatGPT account credentials were compromised and listed for sale across multiple dark web platforms.

The figures have only grown from there, along with product variety. Beyond stolen accounts, purpose-built malicious AI tools have emerged. Tools like WormGPT and FraudGPT are marketed through underground forums and Telegram channels, offering capabilities such as writing malicious code, identifying vulnerabilities, and generating phishing pages — all without the ethical guardrails of mainstream platforms. The pricing varies widely. Premium access to AI platforms like ChatGPT can sell for anywhere from roughly €8 to €500, depending on usage limits, and automated services can generate up to 1,000 fake accounts per day using stolen personal data.

There are multiple reasons for the growing demand for unofficial access to AI accounts. One of the most prominent ones is evasion of sanctions. In countries like Russia, Iran or North Korea the access to some of the most popular AI tools has been restricted by blocking local payment options, for example. The dark web marketplaces thus allow users to circumvent the restrictions through the use of VPNs and cryptocurrencies. They can also be used to obfuscate the real user of the service. Many of the offers promise full access to the API of the AI, allowing users to ignore any guardrails preventing malicious behaviour such as cybercrime. As those accounts are usually stolen, any costs are billed to the victim, not the user.

The implications are serious on multiple fronts. Compromised credentials can grant attackers access to corporate AI environments, potentially exposing customers' personal and financial information, proprietary intellectual property, and other sensitive data. In a worst-case scenario, access to a corporate AI account could even facilitate a larger intrusion to the organisation's systems. If the settings for the AI are not securely configured, an attacker could use the tool to inject malware or escalate privileges. Ignoring all that, the fact that more people are willing to pay for the accounts means that the profitability of stealing them has increased, which in turn is enough to attract a growing number of criminals to try and profit from the situation.

Defending against these threats requires a multi-layered approach. Monitoring employees' AI usage, implementing passkey-based or multi-factor authentication for AI platforms, and employing dark web monitoring services to detect stolen credentials early are all important steps in preventing threat actors from using a corporation's own AI accounts against it. The bottom line: as AI becomes more central to business operations, so does securing access to these platforms — it's a critical part of any organisation's cybersecurity posture.

REFERENCES:

Events in the Cyber Landscape

https://thehackernews.com/2026/03/openai-patches-chatgpt-data.html

https://techcrunch.com/2026/03/18/meta-is-having-trouble-with-rogue-ai-agents/

https://www.theguardian.com/technology/2026/mar/20/meta-ai-agents-instruction-causes-large-sensitive-data-leak-to-employees

https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300

https://www.cybersecuritydive.com/news/citrix-netscaler-exploitation-vulnerabilities/816097/

https://therecord.media/cisa-tells-federal-agencies-to-patch-citrix-netscaler-bug

https://yle.fi/a/74-20218659

https://www.mtvuutiset.fi/artikkeli/wsj-iraniin-kytkeytynyt-ryhma-teki-historian-merkittavimman-sota-ajan-kyberiskun/9311120

https://www.reuters.com/world/china/eu-sanctions-chinese-iranian-companies-cyber-attacks-2026-03-16/

https://www.reuters.com/world/europe/russia-backed-hackers-breach-signal-whatsapp-accounts-officials-journalists-2026-03-09/

Key Personnel are not Immune to Russian Phishing

https://www.bleepingcomputer.com/news/security/dutch-govt-warns-of-signal-whatsapp-account-hijacking-attacks/__

https://therecord.media/russian-hackers-target-signal-whatsapp-warn-dutch-intelligence-agencies__

https://therecord.media/russia-iran-cyber-fbi-hacks__

https://www.bleepingcomputer.com/news/security/fbi-links-signal-phishing-attacks-to-russian-intelligence-services/__

https://www.cert.ssi.gouv.fr/uploads/20260320_NP_C4_Alerte_Ciblage_messagerie_instantanee.pdf

https://www.politico.eu/article/russian-hackers-snoop-ukrainian-signal-accounts-google-report/

Cybersecurity-based US Router Ban will Lead to Weaker Cybersecurity

https://reason.com/2026/03/25/fcc-bans-nearly-all-wireless-routers-sold-in-the-u-s/

https://www.aarp.org/personal-technology/fcc-foreign-router-ban-explainer/

https://www.fcc.gov/document/fcc-updates-covered-list-include-foreign-made-consumer-routers

https://www.reuters.com/sustainability/boards-policy-regulation/fcc-banning-imports-new-chinese-made-routers-citing-security-concerns-2026-03-23/

Claude's Ability to Understand Old Programming Languages is a Security Threat

https://claude.com/blog/how-ai-helps-break-cost-barrier-cobol-modernization

https://www.linkedin.com/feed/update/urn:li:activity:7436235669938614272/?originTrackingId=1epJL9ZY7DcKI2LBHV6BNQ%3D%3D

Claude Sonnet 4.6

Demand for Stolen AI Accounts Increases Criminals' Interest in Credential Theft

https://www.bleepingcomputer.com/news/security/paid-ai-accounts-are-now-a-hot-underground-commodity/

https://outpost24.com/blog/dark-ai-tools/

https://www.csoonline.com/article/3479476/hottest-selling-product-on-the-darknet-hacked-genai-accounts.html

https://www.group-ib.com/media-center/press-releases/stealers-chatgpt-credentials/

Cyberwatch MONTHLY REVIEW

PUBLISHER Cyberwatch Finland | Nuijamiestentie 5 C, 04400 Helsinki | www.cyberwatchfinland.fi

THREAT INTELLIGENCE REVIEW

Cyberwatch Finland publishes threat intelligence monitoring that collects the most significant cyberattacks of the past month and information on the most active and upcoming threat actors around the world. Cyberwatch analysts monitor activity not only on the surface network, but also on the deep and dark web. The sources also include publications by international information security actors and extensive monitoring of the Finnish and international media field.

Major Cyberattacks and Campaigns

Data breaches reported by month from last twelve months. Source: Cyber Intelligence House

(Note: The graph does not take into account, for example, denial of service attacks, but only data breaches where data has been proven to have been leaked)

EUROPEAN COMMISSION DATA BREACH

DATE: 24.3.2025
DESCRIPTION: The European Commission announced that it had encountered a cyberattack that targeted the Commission's Amazon Web Services (AWS) user accounts. This is already the second cyberattack experienced by the European Commission in a month. The last time, its mobile device management platform was hit by a cyberattack at the turn of February and March.
THREAT ACTOR: ShinyHunters. The Commission itself has not confirmed the attribution.
MOTIVE: Unknown.
IMPACT: The Commission is still investigating the case, but the ShinyHunters cybercrime group, which claimed responsibility for the attack, said that it has obtained 350 gigabytes of data from the Commission's AWS database. The attackers claim that at least employee data is included, but there may also be other information that has been leaked.

PUERTO DE VIGO RANSOMWARE ATTACK

DATE: 24.3.2026
DESCRIPTION: Puerto de Vigo, a port on Spain's Atlantic coast, suffered a ransomware attack. The port is an important connecting point for vehicles, vehicle logistics, fish and metal. The port transports cargo especially to China and South and North America.
THREAT ACTOR: Unknown.
MOTIVE: Financial

IMPACT: A ransomware attack stopped some of the port's digital systems. Among other things, the logistics management systems went down, and the port therefore switched partly to paper and pen in order to keep the port operational. The attack once again underlines the cyber threats to critical infrastructure globally.

PUERTO RICO DEPARTMENT OF TRANSPORTATION CYBERATTACK

DATE: March 2026
DESCRIPTION: The Puerto Rico Department of Transportation suffered a cyberattack. Puerto Rican government agencies and institutions have been the target of constant cyberattacks, especially during the past year.
THREAT ACTOR: Unknown
MOTIVE: Unknown.

IMPACT: Department of Transportation was forced to close some of its functions due to a cyberattack. For example, driver's license, permit and vehicle registration services had to be kept out of service after the attack targeted their information systems. All appointments for these services were also cancelled, and the booking of new appointments was suspended.

FBI DIRECTOR'S EMAIL HACKED

DATE: 27.03.2026
DESCRIPTION: The personal email of Kash Patel, the director of the US Federal Bureau of Investigation (FBI), was hacked and its contents were shared on the website of an Iranian hacker group.
THREAT ACTOR: Handala. It is an Iranian hacker group that has recently distinguished itself as a perpetrator of cyberattacks in the context of the Iranian war. In addition to hacking Patel's email, the group was behind the data breach of hospital equipment manufacturer Stryker, among other things.
MOTIVE: Political

IMPACT: FBI Director Kash Patel's personal Gmail account was hacked, and the attacker published pictures, documents and conversations on the website of the Iranian hacker group Handala. The group cited the FBI's operations against Handala and the sinking of an Iranian warship in the Indian Ocean as reasons for the attack. With this attack, Handala sought to embarrass the FBI publicly, stating on their website that "the FBI is just a name with no real security behind it" and "What can be required of lower-level FBI employees if their director is so vulnerable to breaches."

Active and Rising Threat Actors

BEARLYFY

DESCRIPTION: Bearlyfy is a pro-Ukrainian hacker group that has directed its attacks against Russian companies.
RECENT ACTIVITY: First observed in 2025, the hacktivist/cybercriminal group Bearlyfy has already carried out over 70 cyberattacks against Russian organisations. Victims have included consulting and industrial companies. Bearlyfy does not publicise its own activities and does not, for example, maintain a "shame list" of victims typical for ransomware actors.
METHODS AND TACTICS: Bearlyfy is an ideologically motivated hacker group that seeks to cause maximum damage to Russian organisations. In addition to this disruptive activity, the group is also motivated to collect as much money as possible through its attacks, partly to develop its own operations. This development trajectory has already been observed. Initially, the group was known for its hastily assembled attack tools. The group essentially purchased ready-made tools from cybercriminal marketplace platforms and leveraged the support of like-minded hacktivist groups in its attacks. In recent times, the group's tools and methods have been observed to have matured, and the amateurish early-days operations are long gone. As many as one in five of the group's victims have paid the demanded ransom. The initially smaller ransom demands have already risen to hundreds of thousands of euros. In its attacks, Bearlyfy has frequently exploited user accounts created for the victim organisations' subcontractors or various third-party organisations with trusted links to the target network. Using these compromised credentials, Bearlyfy deploys data-encrypting malware into the victim's systems. After encryption, it threatens to destroy the entire victim's information system using data-wiping malware if the ransom is not paid.

HANDALA

DESCRIPTION: Handala is an Iranian hacker group that multiple sources have linked to Iran's Ministry of Intelligence and Security (MOIS).
RECENT ACTIVITIES: Handala has recently struck targets including the FBI director's personal email account, as well as the US-based global healthcare company Stryker, destroying Stryker's information systems around the world.
METHODS AND TACTICS: Handala frequently exploits supply chain vulnerabilities in its attacks. In the early stages of an attack, it focuses on the victim's IT service provider in order to gain access credentials to the victim's systems. Handala commonly uses its own data-destroying malware, "Handala Wiper," or data-encrypting software in its attacks. Depending on the target, the group typically aims either to destroy target systems or to steal and publish critical information from them.

AKIRA

DESCRIPTION: A cybercriminal group first encountered in March 2023. Operates on a Ransomware as a Service (RaaS) model.
RECENT ACTIVITY: During March 2026, Akira has been linked to approximately 140 cyberattacks globally. Its most recent victims include technology companies, law firms, employment platforms, and food production companies. Akira has long been one of the most well-known and active cybercriminal groups.
METHODS AND TACTICS: 80% of Akira's victims are small or medium-sized businesses primarily from North America or Europe. Akira uses so-called double extortion in its operations; it steals the victim's data, encrypts it, and threatens to publish the data if a ransom is not paid.

ANUBIS RANSOMWARE

DESCRIPTION: A Russian speaking Ransomware as a Service (RaaS) group first observed in late 2024.
RECENT ACTIVITY: Anubis has become significantly more active during March. According to data from Cyber Intelligence House, Anubis had 24 confirmed victims during March, compared to just three in December 2025 and none during January and February 2026. Among the most recent victims are a French IT company and a US law firm.
METHODS AND TACTICS: Anubis offers ransomware tools to other cybercriminals through affiliate agreements under three different models. It provides its malware to partners by retaining 20% of the profits for itself. For providing data theft tools, the group retains 40%. In collaborative operations — where Anubis offers assistance, such as gaining access to the victim's systems — it retains 50% of the operation's overall gains. Especially in this last method, Anubis has set several rules regarding victim targeting, such as that the victim must be located in North America, Europe, or Australia, and the victim must not be a representative of the education, government, or nonprofit sectors.

Cyberwatch Finland

Cybersecurity Capacity Building

We serve our customers by strengthening and developing their cybersecurity culture. Our goal is to improve strategic cyber capabilities at all levels of operations, from individuals to the top management of organisations.
We inform the public about current cybersecurity phenomena and the factors affecting them.

1. STARTING POINT
- Cyber matuCheckingrity
- Web analysis and attack surface analysis
- Operational environment analysis

2. ESTABLISHING OPERATIONS
- Cybersecurity Act measures & guidelines
- Risk management plan
- Cyber policy paper
- Utilizing the expertise of partners: e.g. cybersecurity guidelines and vendor assessments

3. TRAINING FOR MANAGEMENT AND STAFF
- Producing information about cybersecurity through training while operations are ongoing
- Operational environment analysis: weekly and monthly review
- Scenario training with the customer

4. MONITORING
- Maintaining situational awareness through continuous monitoring and providing additional training as needed
- Investigating the security of supply chains and conducting a risk analysis/web analysis

5. SUPPORTING DEVELOPMENT
- Management Consulting Services
- Supply Chain Auditing
- Background Investigations
- Cyber Due Diligence
- Annual scenario exercise on current cyber threats and how to prepare for them

6. CONTINUITY MANAGEMENT
- Continuity management
- Personnel training
  -> in the form of operational environment service recordings and/or according to wishes

Operational Environment Analysis

Cyberwatch's analysis team constantly monitors the cyber-security operational environment by collecting and analysing information about events, phenomena and changes in the cyber world. Situational awareness is produced by regular situational reviews.

You can now order a 3-month trial period at a discounted price!

More information: info@cyberwatchfinland.fi

WEEKLY REVIEW

Weekly reviews introduce the current events of the cyber world. The focus of the weekly review is in identifying phenomena and trends and placing them in a relevant framework. The weekly reviews serve as the basis for the monthly reviews and the annual forecasts that are based on this data. With the help of the weekly reviews, it is possible to get an up-to-date understanding of significant events in the cyber world to support decision-making. The weekly reviews are published 52 times a year in Finnish and English.

CYBERWATCH MAGAZINE

Cyberwatch magazine is a digital and printed publication, in which experts from both inside our organisation and from our professional network explain the current events of the cyber world, the development of technology and legislation, and their impacts on society, organisations and individuals.

MONTHLY REVIEW

The monthly review examines previous and current month's the most significant cyber events, phenomena-, and trends including their interdependencies, while also tying them into a broader framework. The monthly review is divided into three parts: the most significant cyber events of the month; phenomena that should be highlighted; and entities whose development is worth following. With the help of the monthly review, it is possible to get a deeper insight into how the events of the cyber world affect society and the operational environment. The monthly reviews are published 12 times a year in Finnish and English.

SPECIAL REPORTS

We produce reports and overviews on customised themes, for example from a specific industry or target market: assessments of the current state, threat assessments, analyses of the operational environments, and forecast.

Web Analysis - darkSOC®

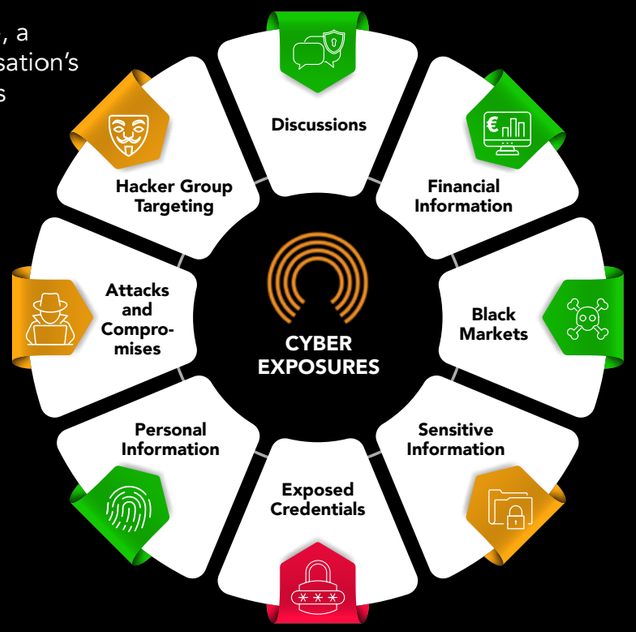
WEB ANALYSIS

DarkSOC® dark and deep web analysis

- DarkSOC® analysis reveals the organisation's profile and level of exposure in the dark and deep web.
- Data is collected on servers located around the world non-stop at 9 Gb per second.
- The analysis can reveal, among other things, shortcomings in the organisation's cybersecurity, leaked information and other potential problems.
- The analysis provides insight into what the organisation looks like through the eyes of cybercriminals and hostile actors.

Attack surface analysis

- In the attack surface analysis, the structure of the organisation's network infrastructure and the state of its cybersecurity are analysed in six different groups of risk factors.
- In terms of the attack surface, a depiction of what the organisation's network looks like in the eyes of an external observer is reported.
- The parts of the network assets related to the organisation, such as servers, open ports, applications and websites are listed.
- The findings are divided into eight categories and three levels based on severity.
- The most important findings are reported in an executive summary report to support decision-making.
- The main report includes a more detailed presentation of the findings, as well as recommendations for corrective actions and strategic-level development targets.



MONITORING

Based on the analysis, monitoring is agreed upon to determine the effectiveness of the measures and to detect new threats. New findings observed during monitoring are examined in relation to previous observations and the reasons why the number of observations has changed are analysed. The results are reported at agreed intervals.

- Regular monitoring: a report delivered at agreed intervals, for example monthly, quarterly, biannually or annually.
- Continuous monitoring: 24/7 monitoring of new findings, and the reporting of information directly to the customer

Security of the Supply Chain

THE NIS2 EU-DIRECTIVE (Network and Information Security Directive 2) COMPLIANCE REQUIRE

Company policies needs to give attention to security around supply chains and the relationship between the company and direct supplier. Companies must choose security measures that fit the vulnerabilities of each direct supplier. And then companies must assess the overall security level for all suppliers.

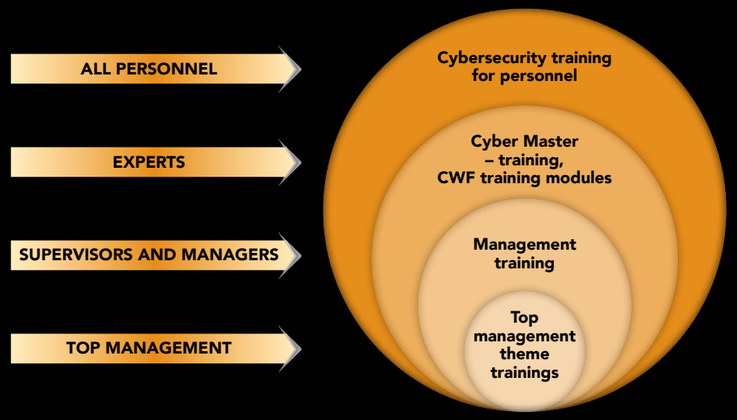
The analysis can be done for selected parts of the supply chain organisations (requires an agreement). The findings of the attack surface analysis are introduced to the concerned organisations which are responsible for the implementation of corrective actions and reporting to the customer when the corrective measures have been taken.

An example of service content:

- Preliminary analysis for the supply chain
- Web analysis for the supply chain
- NIS2 implementation training

Auditing the cybersecurity practices of the supply chain increases the customer organisation's cyber maturity and helps the company better meet the minimum requirements of the Cybersecurity Act. It can, for example, enable the customer to determine the cyber maturity of potential partners and to conduct a risk assessment in a corporate acquisition situation.

Training and Competency Development



CYBERWATCH TRAINING MODULES AND LECTURES

We also provide customized training modules and lectures for your organisation, which will help you strengthen your cybersecurity skills and prepare you to face the changing challenges of our digital operating environment.

Our training offers consists of module packages and individual lectures, from which you can choose the parts that best suit your organisation's situation or operations. The training can be delivered either as face-to-face training, hybrid training or online courses. In addition to training and lectures, you can also order scenario-based training for your organisation, which will help you to collect and structure information required for understanding the future as comprehensively as possible.

Examples of training modules:

Module 1: Cybersecurity Management
Module 2: NIS2 and Cyber Regulations
Module 3: Cybersecurity Process
Module 4: Cyber Risks and Contingency Planning
Module 5: OT Security
Module 6: Hybrid Influence and Cyber Warfare
Module 7: Cybercrime
Module 8: Cyber-Secure Society
Module 9: Critical Infrastructure Protection
Module 10: The ABC of Cyber Definitions

Examples of lectures:

- Cybersecurity of the Energy Sector
- Cybersecurity of the Logistics
- Cybersecurity of the Satellites and Positioning Systems
- Cybersecurity of the Critical Infrastructure
- Cybersecurity of the Health Sector
- Cyber Warfare and the Impact of the War in Ukraine on the Cyber Environment
- Cybersecurity Management and Crisis Communication
- Cyber Hygiene
- Cybercrime
- Dark Web

CYBER SITUATIONAL AWARENESS FOR PERSONNEL

The Cyber Security Act (NIS2) that has come into force and the cyber risk management obligation that came with it require that organisations' personnel must be regularly provided with training, that aims to:

1) improve awareness of cybersecurity in general,
2) develop cyber hygiene practices and
3) increase understanding and awareness of current cybersecurity risks.

The cyber situational awareness training for personnel meets this requirement. The content consists of significant cyber phenomena discussed in the weekly and monthly reviews during the previous month. The training is held once a month for personnel as a live stream or other remote training and lasts approximately 60 minutes.

MIF TRAINING PROGRAMS

We are producing Cyber Master specialised vocational qualification training together with the Management Institute of Finland (MIF Oy). Currently, the training programs offer the Cyber Master Basics and Cyber Master Extended training modules. The purpose of the training is to deepen the understanding of cybersecurity threats and provide practical tools to protect the organisation's operations.

Cyber Master Basics

The aim of the course is to learn the basics of cybersecurity and to build your own organisation's resilience. The Cyber Master training deepens your understanding of cybersecurity threats and provides practical, non-technical tools to protect your organisation's operations. In the training, you will learn how to build an organisation's ability to tolerate disruptions and manage crisis situations.

Content of the Training:

- Operating environment and leadership
- Cyber risk management
- Cyber resilience

Cyber Master Extended

The aim of the advanced course is to strengthen the participants' cybersecurity expertise and take your organisation's cybersecurity to the next level. The Cyber Master Extended training offers a more in-depth approach to cybersecurity, helping you develop your organisation's resilience and ability to manage cyber threats together with your management. The training is designed for those who want to take cybersecurity to a strategic level and lead the organisation's development holistically.

Content of the Training:

- Deepening cyber leadership and protecting operations
- Cybersecurity planning and development

CURRENT COURSE CONTENT

OUR COURSES' CONTENT, ALSO AVAILABLE ON CYBER MASTER BASIC

Training day 1

Theme:
Operating environment and management

1. Operating environment
2. Personnel related Cybersecurity
3. Regulatory effects
4. Cybersecurity Management

+ Assignments

Training day 2

Theme:
Cyber risk management

1. Cyber risk management
2. Cybercrime
3. Technological development
4. Security of Operational Technology

+ Assignments

Training day 3

Theme:
Cyber resilience

1. Cybersecurity Planning
2. Continuity management
3. The company's cyber culture and expertise
4. Case analyses

+ Assignments

TRAINING DAY COVERS FOLLOWING ISO27001 REQUIREMENTS:

Training day 1:
4 Context of the organisation
5 Leadership

Training day 2:
6 Planning

Training day 3:
8 Operation
7 Support
(9 Performance evaluation)
(10 Improvement)

OUR COURSES' CONTENT, ALSO AVAILABLE ON CYBER MASTER EXTENDED

Training day 1

Teema:
Cybersecurity preparedness

1. Cybersecurity Management
2. Cybersecurity preparedness
3. Risk management and identification
4. Identity and Access Management (IAM)

+ Development project +assignments

Training day 2

Teema:
Kyberturvallisuuden vaste

1. Attack detection and response
2. Recovery of cybersecurity
3. Quantum technology
4. The change of Cybersecurity

+ Assignments

TRAINING DAY COVERS FOLLOWING NIST FUNCTIONS:

Training day 1:
Govern, Identify, Protect

Training day 2:
Detect, Respond, Recover

Cyber Risk Management Model

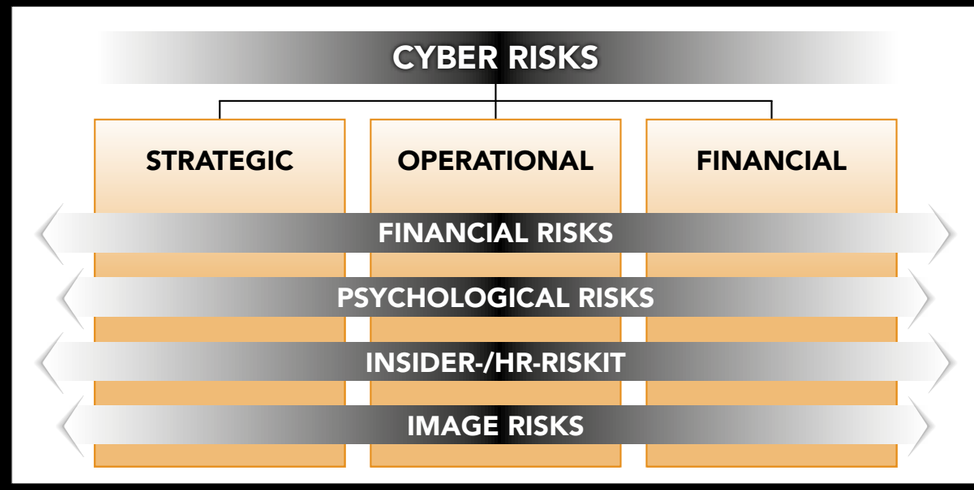
Cybersecurity needs to be increasingly considered in different stages of the business plan. A comprehensive cybersecurity risk management plan will provide a roadmap for how to better address cybersecurity threats and implement the required actions brought by the increasing EU regulation and national legislation.

The plan covers the four components of cybersecurity: management, technical solutions, training personnel, and operational processes.

The cyber risk management model process consists of four stages:

1. **Defining the starting point**
2. **Cyber risk analysis**
3. **Cyber risk management model**
4. **The result is a functional and proactive cybersecurity system**

STARTING POINT	ANALYSIS	MANAGEMENT MODEL	RESULT
1. Cyber maturity of the organisation -> web analysis 2. Cyber threats and risks of the business	Cyber risk analysis - Personnel - Technology - Processes Using data generated by web analysis as a basis	Cyber risk management - Monitoring of the threats - Activities: personnel, technology, processes	Cybersecurity system: functional, credible & proactive - Maintains situational awareness - Business continuity management



NIS2 Consulting Service

Cyber Security Directive (NIS2)

Requires that the entities implement appropriate and proportionate technical, operational and organisational measures:

- **To manage the risks** of the security of the network and information systems they use in their operations or services.
- **To prevent or minimize the impact of deviations** on the recipients of their services.

Entities are divided into critical sectors and other critical sectors.

The new Cybersecurity Directive (NIS2) that has come into force has brought new obligations on organisations' digital risk management.
These include, among others:

1) cyber risk management implementation and monitoring
2) registering on the operator list,
3) arranging cyber training for every level of staff,
4) identifying suppliers in the supply chain, and
5) reporting incidents.

WE SUPPORT COMPANIES IN IMPLEMENTING THE NEW LEGISLATION.

We provide assistance with:

1) Organising training:
   - NIS2 implementation training (2 hrs)
   - Cyber situational awareness for the personnel (once / month, 1 hrs)
   - Training modules 1–10, (3 hrs / module)
   - MIF: Cyber Master Basics & Cyber Master Extended (3 day + 2 day)
   - Other Cyberwatch's lectures and online courses
2) Defining and registering your entity:
   - Does NIS2 concern the entity
   - Critical sector or other important sector
3) Cyber risks consultation and in creating a risk management process
4) Checking the security of the supply chain
5) Other NIS2-related questions

We offer a free introduction to the requirements of the Cybersecurity Act!

Management Advisory Services

We are an experienced and trusted advisor and cybersecurity expert. In cyber consulting, the key is to highlight what the management needs to know about the cyber world, its current risks and their impacts for the business.

We support in combating threats, managing cyber risks and ensuring business continuity. We help develop comprehensive security, cybersecurity, internal security and partner risk management. Our working methods include for example theme presentations, memoranda, workshops and scenario work.

Cyber Due Diligence

Cybersecurity due diligence is a process that helps identify and assess cybersecurity-related risks that may affect, for example, a commercial agreement, investment, financing arrangement or the terms of a corporate acquisition. Cyber due diligence also serves as an essential tool in competitive bidding situations between contracting parties.

The Cyber Due Diligence project is composed of a detailed web analysis and "audit process" related to cybersecurity, which includes, among others:

- ✔ Assessment of the current state of cybersecurity and information security
- ✔ Review of the cybersecurity level of third parties
- ✔ Review of the history of information security breaches and potential cyberattacks
- ✔ Review of the cybersecurity culture
- ✔ The assessment of the level of cyber hygiene and cybersecurity training arrangements
- ✔ Responding to cybersecurity regulations and requirements
- ✔ Cybersecurity and information security risk management
- ✔ Integration of cybersecurity culture after a corporate acquisition (NIS2 compliance and coordination of internal policies)

MESSUKESKUS
The real social media

FOR A BETTER DIGITAL FUTURE

Politics, economy, reality and the future of cybersecurity.

Technology, digitalisation, and AI are transforming the global landscape at an unprecedented pace. While this shift creates vast opportunities, it also introduces new vulnerabilities affecting businesses and public administration. Cyber Security Nordic explores the critical role of cybersecurity, providing insights from both corporate and governmental perspectives. Connect with the entire Nordic cyber industry, discover the latest solutions, and experience the first-class programme.

SAFETY & COMPETITIVENESS | EUROPEAN SECURITY | TRUSTED DIGITALISATION & INFORMATION SECURITY | DEMOCRACY & DIGITAL POLICIES

CYBER SECURITY NORDIC

28–29 Oct 2026
Helsinki Expo and Convention Centre

cybersecuritynordic.com