



Cyberwatch Finland

MAGAZINE 2/2026

Cybersecurity
is updating



Cybersecurity is Built by Small Actions and Management of Large Concepts

➤ Our Aim is to Add
Cyber Capabilities
in the World



CONTENT



Editorial

➤ AAPO CEDERBERG



Digital Immune System:
Trust is Earned Every
Day, not Declared Once

➤ REPE HARMANEN



Cyber Security Nordic Brings
Together Decision – Makers
and Experts and Practioners
as Cybersecurity Moves
Beyond the IT Silo

➤ ANU EVELIINA MATTILA



A Capability-Based
Approach to Identifying
and Remediating Cyber-
security Gaps in Critical
Infrastructure

➤ EETU LAAKSO, VESA KUIKKA
& KIMMO K. KASKI



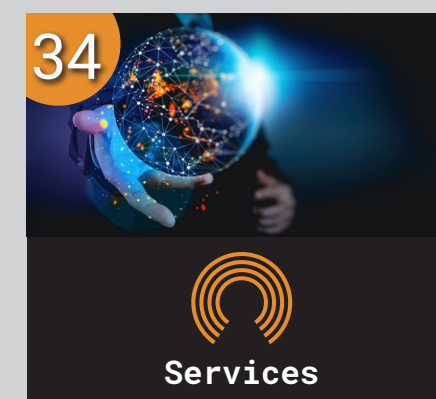
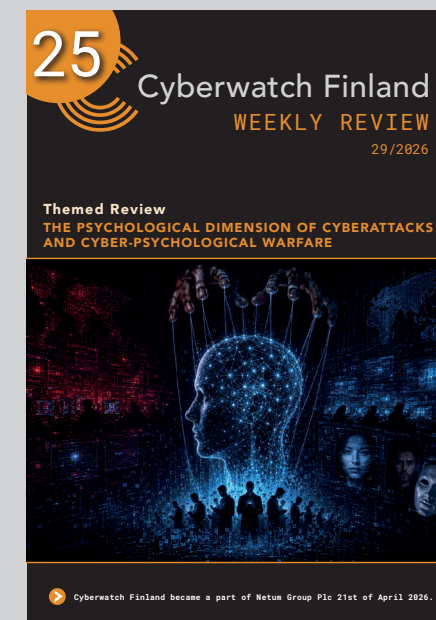
Two Phenomena that
Will Change Everything
About Security

➤ KIMMO ROUSKU



The Importance of Resilience
and Reliability is Becoming
Even More Pronounced as
Cybersecurity Transformation
Trends Intensify

➤ RISTO RAJALA
& PETER SUND





The global security environment is changing faster than ever. The superiority of the superpowers is being challenged by smaller states and actors. It is evident, that wars can no longer be won with military power only, as the conflicts in the Middle East and the war in Ukraine vividly illustrate. Asymmetric methods, new technologies and operational measures have succeeded in challenging the traditional use of military force and superiority, even though such force still possesses immense destructive power and the capacity to inflict human casualties. Conflicts are becoming prolonged, causing ever greater losses and economic damage, both to the parties involved and to bystanders. Various interdependencies keep throw-

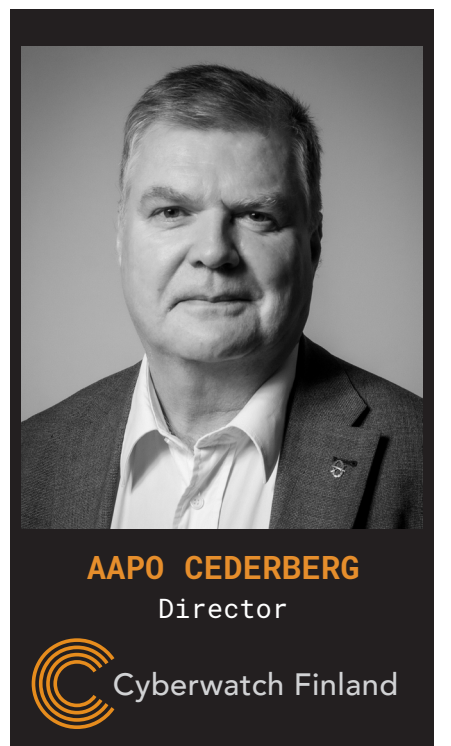
ing up surprises — as the closure of the Strait of Hormuz demonstrated, difficulties arose for the entire global economic system. The future looks increasingly uncertain, and the number of local conflicts appears to rise. Their forms, substance and effects will continue to cause unwelcome surprises in the times ahead.

In an unstable world we must be stronger than ever and choose our allies and partners with greater care. This historical truth does not appear to be changing, whether it concerns relations between states or the logic of business. That is precisely how we at Cyberwatch Finland have been thinking too. We are too small to do everything alone, and success calls for stronger financial resources and

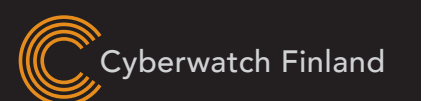
more skilled staff. Adopting AI on its own is not enough — safe and intelligent “AI-tisation” requires additional resources during this period of transformation. The faster pace of renewal and the capacity for innovation are becoming invaluable. We gain all of this by joining the Netum Group. The synergy benefits are apparent, and Cyberwatch’s intelligent cybersecurity services provide a solid foundation to build a new, winning cybersecurity concept for Netum. The company is full of skilled experts, and investment in the controlled use of AI forms part of our shared strategy. We are delighted to adopt Netum’s slogan “Inspired by wisdom”, as it fits well with our own thinking and way of working.

There is a great deal of talk about the transformation of the cyber world, yet global uncertainty makes it far from easy to identify the drivers of that change. Everyone understands that AI and quantum technologies are part of this transformation, but there are already many differing views on their effects and possible applications. Only change itself, and its pace, seem certain. Digitalisation and its associated technologies will remain the cornerstone of a competitive welfare state. In a turbulent world, reaping the benefits of digitalisation calls for greater investment in cybersecurity. That is why intelligent, cost-effective cybersecurity services and technologies will only become more and more important.

On its own, EU-driven regulation does not guarantee better cybersecurity services, but it serves as a useful wake-up call for all critical actors of society as to the importance of the matter. We have done many things right, and certain patterns of the cyber world are not about to change. A winning concept will continue to be built on people’s competence, intelligent technologies and secure working practices. This concept provides a sound basis for developing Netum’s cybersecurity services, and it is where we want to invest — and to do so wisely and inspired by wisdom. As threats and risk factors change, cybersecurity must become ever more agile and intelligent. In this shift in security culture, we must keep our pace and must lead the way ahead.



AAPU CEDERBERG
Director





REPE HARMANEN,
NETUM GROUP PLC

DIGITAL IMMUNE SYSTEM: Trust is Earned Every Day, not Declared Once

Cybersecurity is no longer just a technical control or a periodic compliance exercise. It is the organisation's ability to remain operational, prove its resilience, and earn customer trust every day. In a digital society, trust does not come from assuming that nothing will ever break. It is created by the fact that critical service continues even when something breaks.

The threat level has risen permanently

The state of cybersecurity in Finland remains serious, with no signs of easing. According to the Finnish Transport and Communications Agency Traficom's Cyber Security Centre's 2025 review, the number of severe cybersecurity incidents has remained at a record high level for the past two years. The year 2026 marks a clear turning point: artificial intelligence

is enhancing the capabilities of both attackers and defenders, making the operating environment faster-paced, broader in scope, and increasingly difficult to predict.¹

Deepfake phone calls can already sound convincingly like a manager or colleague. Phishing messages are written in flawless Finnish. Cybercrime has evolved into a service-based business model, and Ransomware-as-a-Service has become part of the everyday threat land-

scape. Meanwhile, the number of destructive malware attacks continues to grow steadily.²

The traditional way of thinking about cybersecurity, where you build a wall, buy a licence and run an audit every three years, is no longer enough. The threat field does not follow our schedules. It is constantly adapting, and we must adapt with it.

In this article, I would like to introduce an alternative framework. An organisation's cybersecurity works best when it resembles a biological immune system: it recognises exposure, responds to threats, and learns from every encounter. Its purpose is not to prevent every attack; that is impossible. Its purpose is to ensure that the organisation can withstand attacks, recover from them, and continue operating stronger than before.

The law no longer asks: Is it protected? It asks: Can you prove resilience?

2026 will be a crucial year for the implementation of European cyber law. NIS2 Directive⁶ is in full force and the DORA Regulation⁵ has been applied to the financial sector since January 2025. The change is real: cybersecurity has become legalised.

The current transition bears a strong resemblance to the arrival of GDPR. Back then, many organisations believed they could get by with a reactive approach, but many quickly discovered that was not enough. Today, businesses are expected to demonstrate their resilience on demand, under the threat of significant sanctions. In cybersecurity, the focus is shifting from promises to proof.³

"Compliance with DORA and NIS2 is not merely a regulatory obligation but a strategic opportunity to build and sustain digital trust."

– ISACA, 2025⁴

The NIS2 Directive applies to a wide range of sectors, from energy and healthcare to transport and public administration. Penalties can reach up to €10 million or 2% of global annual turnover. And responsibility lies with senior management—not the IT department.⁶

At the same time, discussions on the reform of Finland's Emergency Powers Act have brought three requirements into focus: operators of critical functions must be able to plan, exercise, and allocate resources for exceptional situations. Not as standalone initiatives, but as a continuous cycle. This mirrors precisely the expectations set by NIS2 and DORA for cybersecurity. A digital immune system cannot emerge without continuous practice.

The immune system recognises: exposure is everywhere

We repeatedly encounter the same mistake: data protection, cybersecurity and the continuity of IT services are procured as separate projects. They are not separate. They are layers of the same immune system, and the system is only as strong as its weakest layer. The weakest link is not necessarily your own system, but the subcontractor, the integration interface or the partner's information security level.

Layer 1: Data protection – the protection of personal data is a fundamental right

The GDPR obligations are familiar, but actually complying with them is becoming more complicated every year. The rise of artificial intelligence further increases the pressure: the data protection and information security requirements of AI-based systems require precise internal guidance.⁹ At Netum, our public sector clients remind us of this every

day. When an appointment system, patient record, permit process, or public service stops working, it is not merely a technical disruption. It is a disruption of trust.

Layer 2: Cybersecurity – the visible and invisible threat surface

Cyberattacks are no longer aimed solely at organisations directly. They target the weakest links: supply chains, subcontractors, and integrations. An organisation's digital immune system does not end at its firewall. It extends into the supply chain, subcontractor networks, integrations, and the operational resilience of partners.¹⁰

The darkSOC analysis developed by Cyberwatch Finland provides a view of an organisation's exposure level, also in the dark and deep web. Data is constantly collected from hacker forums, data breach sharing platforms, and dark web marketplaces, up to 9 gigabytes per second, around the clock.⁸ This creates a picture of what the organisation looks like through the eyes of a hostile actor. Knowing where you are exposed is a very different starting point from discovering it after an attack.

Layer 3: Continuity of IT service – operations must not stop

This layer is the one that is most underestimated. Critical infrastructure, the public sector, and healthcare are the backbone of society, and the interruption of their services is not merely a technical disruption but a serious matter.⁷

DORA requires continuous monitoring of ICT systems, anomaly detection mechanisms, and tested resilience.¹⁰ 24/7 monitoring, proactive updates, and a rehearsed con-

tinuity plan are not luxuries. Their value becomes visible precisely when everything else starts to fail. This is how the digital immune system reacts.

**Netum + Cyberwatch
Finland: Embedding
cybersecurity as part
of trust leadership**

Cyberwatch Finland's integration into Netum was no coincidence.⁹ For us, cybersecurity and data protection are not add-ons, but a strategic cross-cutting strength. This is particularly important as we grow in data, integration and artificial intelligence solutions and expand into the private sector.

Cyberwatch Finland brings Netum the ability to view cybersecurity from the perspectives of management, regulation, risk, supply chain,

and continuity.⁸ This complements Netum's technical delivery capability: we don't just build systems, we help our customers ensure they can withstand pressure. Our services span from situational awareness and darkSOC analysis to Cyber Due Diligence assessments in corporate transactions.

Aapo Cederberg, the founder of Cyberwatch Finland, sums it up well:

"Sustainable cybersecurity starts with top management – where cyber risk management is an essential part of good governance and corporate responsibility."

It is easy to agree with this. In the future, investors, customers and authorities will not only ask what the organisation says it protects. They ask what it can prove, test, and verify. Meeting the minimum requirements is not enough.

**Immune System Remembers
and Strengthens: ISO
27001 and National
Facility Security
Clearance**

For us, ISO 27001 is not a framed certificate on the wall, but the foundation of our digital immune system. It covers all of the group's solution businesses.⁹ It means a documented, audited and constantly evolving way of managing information security, not a single certificate on the shelf. Certification has been maintained uninterrupted for more than two decades.

The National Facility Security Clearance certificate, on the other hand, demonstrates that we meet the authorities' requirements for processing classified information. In public sector procurement, it is concrete evidence that the confidentiality, integrity and availability of information have been prop-

erly managed. Not a promise, but a proven fact.

At Netum, information security is not just a matter for the IT team. The entire staff is trained annually, and the operating models for reporting information security incidents are clear. It is part of the culture.⁹

CWF's expertise in management training, scenario training and risk management further strengthens this culture. The digital immune system is strengthened when the entire organisation trains, learns and remembers.

**Digital Immune
System and Practical
Conclusions**

The biological immune system is not a wall. It detects exposure, reacts to threats, recovers from disruptions, and becomes stronger with each encounter. This is exactly what is now required of organisations.

The digital immune system is not a single technology, standard or service. It is a way to lead trust. The organisation that has it can:

- identify their exposure levels, even in an invisible network,

- react to threats before they materialise into disruptions,
- continue its service provision in the event of a disruption,
- demonstrate its resilience to authorities, customers and investors.

These are not only technical capabilities. They are leadership capabilities. They are also competitive advantages because they are built before they are needed.

For a responsible organisation, the question is no longer about meeting the minimum regulatory requirements. The question is whether it can look its customers, authorities, and investors in the eye and demonstrate that we are prepared, we have trained for this, and our services can withstand disruption.⁸

At Netum, we respond to this through our own operations. Our ISO 27001-based management system, our National Facility Security Clearance, and Cyberwatch Finland's strategic cybersecurity expertise together form a digital immune system that detects, responds, and strengthens over time. Trust is not built on the absence of failure. It is built on services that endure disruption, recover, and grow stronger.

REFERENCES/SOURCES

- 1 Traficom / Kyberturvallisuuskeskus: "Kyberturvallisuuden vuosi 2025 – uhkataso pysyi kohonneena, vakavien tapausten määrät kasvavat". Published on 29 January 2026. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuden-vuosi-2025-uhkataso-pysyi-kohonneena-vakavien-tapausten-maarat>
- 2 Elisa Yrityksille: "Kyberturvallisuus 2026: yhdeksän havaintoa Suomesta". Published on 29 October 2025. <https://yrityksille.elisa.fi/ideat/kyberturvallisuuden-trendit-vuonna-2026-ai-vastaan-ai-ja-8-muuta-havaintoa/>
- 3 DPO Consulting: "ISO 27001, NIS2 and DORA: Building Sustainable Cyber Compliance in 2026". Published on 4 February 2026. <https://www.dpo-consulting.com/blog/iso-27001-nis2-and-dora-building-sustainable-cyber-compliance-in-2026>
- 4 ISACA: "DORA and NIS2: Connection Points and Key Differences". Published on 5 June 2025. <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/dora-and-nis2-connection-points-and-key-differences>
- 5 Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience requirements for the financial sector (DORA). Applicable from 17 January 2025.
- 6 Directive (EU) 2022/2555 of the European Parliament and of the Council on the security of network and information systems (NIS2). Transposed into national law 2024–2025.
- 7 NetNordic: "Pilvipalvelujen turvallisuus vuonna 2026: hallinta, vaatimustenmukaisuus ja jatkuvuus". Published on 25 February 2026. <https://netnordic.fi/insights/pilvipalvelujen-turvallisuus-vuonna-2026/>
- 8 Cyberwatch Finland: Company presentation and service descriptions 2025. <https://www.cyberwatchfinland.fi>
- 9 Netum Group Plc: Annual report 2025. Published in March 2026. <https://www.netum.fi/en/for-investors/>
- 10 ISACA: "Resilience and Security in Critical Sectors: Navigating NIS2 and DORA Requirements". White paper 2025. <https://www.isaca.org/resources/white-papers/2025/resilience-and-security-in-critical-sectors-navigating-nis2-and-dora-requirements>



AUTHOR:



REPE HARMANEN
CEO
Netum Group Plc

Repe Harmanen is the CEO of Netum Group Plc. Netum is a Finnish IT services company that helps the public sector and private organisations build a more functional and secure digital society. In spring 2026, Cyberwatch Finland – a strategic cybersecurity expert company founded in 2017 – became part of Netum. This article emerged from the inspiration of that integration.



➤ ANU EVELIINA MATTILA,
CYBER SECURITY NORDIC

CYBER SECURITY NORDIC BRINGS TOGETHER DECISION – Makers and Experts and Practioners as Cybersecurity Moves Beyond the IT Silo

Cybersecurity is no longer a standalone IT function; it has become a central component of business continuity, trust and societal resilience. Against this backdrop, Cyber Security Nordic has established itself as a key forum in the Nordic cybersecurity landscape, bringing together decision-makers, experts and solution providers to address the industry's most pressing challenges.

The next edition of the event will take place on 28–29 October 2026 at the Helsinki Expo and Convention Centre.

A distinct position in the European cybersecurity landscape

Within the European cybersecurity event landscape, Cyber Security Nordic occupies a clearly defined position between two distinct types of events. At one end are large-scale global conferences, where size delivers visibility but can dilute the overall narrative. At the other are smaller,

more narrowly focused events with limited scope.

Cyber Security Nordic represents a deliberately designed format that bridges these extremes, combining breadth of perspective with depth of insight while maintaining a coherent and structured overall experience.

“Cybersecurity has moved beyond the IT silo and firmly onto the agenda of business leadership. At Cyber Security Nordic, we aim to build a holistic understanding where technology, risk and market dynamics intersect without hype, grounded in the realities organisations face today,” says Miina Miettinen, Producer of Cyber Security Nordic.

A programme designed to build understanding

Held annually over two days, the event has evolved into a comprehensive platform where content, networking and perspectives come together as a structured ecosystem. In 2026, the event will expand to larger exhibition areas, reflecting growing demand and a widening participant base.

A defining feature of Cyber Security Nordic is its programme design. Content is developed around carefully selected themes and the needs of its professional audience. International keynote speakers, alongside

Nordic experts, contribute diverse perspectives that together form a coherent narrative rather than a series of disconnected sessions.

Trust, quality and openness at the core

The event reflects key characteristics of the Nordic operating environment, particularly in how cybersecurity is discussed and developed.

Trust plays a central role, with organisations placing emphasis on collaboration, information sharing and shared situational awareness. The event supports this by providing a platform for transparent and expert-led discussion.

Focus and relevance guide the programme. Themes are closely aligned with current developments, including the evolving geopolitical landscape, the impact of artificial intelligence, regulatory change and organisational resilience.

Openness defines the atmosphere. The format encourages dialogue and interaction, enabling participants not only to follow keynote sessions but also to engage in meaningful discussions with peers.

From strategy to implementation

Cyber Security Nordic is structured around multiple stages to address different levels of cybersecurity decision-making.

Stage One focuses on strategic perspectives, covering cybersecurity as a geopolitical force, a leadership responsibility and a business risk. It features international keynote speakers and senior leaders, bringing insights that are not commonly available in the Nordic region.

Gold Stage and Scandinum Stage address operational and practical dimensions, including IT/OT environments, cloud dependencies and evolving threat actor techniques. On the second day, the Scandinum

Stage hosts Traficom's Infosec Seminar, providing insights into current threats, regulatory developments and national cyber resilience.

Hacker's Corner adds a practical, hands-on dimension with demos, workshops and live case analyses. Topics include phishing analysis, OSINT techniques, threat modelling and SOC simulations, alongside discussions on ethical considerations.

Together, these elements provide a comprehensive view of cybersecurity across strategic, operational and technical levels.

An ecosystem built on interaction

The exhibition is an integral part of the event, bringing together cybersecurity vendors, experts and organisations in a shared environment. This enables discussions to move seamlessly from high-level perspectives to practical solutions.

For participants, this creates an opportunity to gain a broader understanding of the market, technologies and available approaches, while also building meaningful professional connections.

A platform for long-term impact

Cyber Security Nordic is designed not only as a two-day event, but as a platform that contributes to ongoing dialogue and collaboration within the industry. Initiatives such as the Pitch Finland Cyber Security competition support innovation and provide visibility for emerging solutions with international potential.

A focused and relevant forum

Cyber Security Nordic's position in Europe is defined by its scale, its structured programme design and its open discussion culture.

The event is large enough to bring together key players from across the ecosystem, yet focused enough to maintain the quality of interaction and discussion. Its emphasis on relevance and clarity ensures that participants leave with practical insight, new connections and a clearer understanding of the cybersecurity landscape.

AUTHOR:



ANU EVELIINA MATTILA
Marketing and Communications,
Cyber Security Nordic,
Helsinki Expo
and Convention Centre
(Messukeskus)

Key themes for 2026

The 2026 programme centres on three overarching themes:

- **Resilient business and crisis preparedness**, including business continuity, supply chain risks and the implementation of NIS2 and DORA
- **Cybersecurity, defence and the European security landscape**, addressing geopolitical developments and hybrid threats
- **Trusted digital society and democratic security**, focusing on disinformation, AI-related risks and trust in digital systems

These themes reflect the expanding role of cybersecurity as both an economic and societal issue.

EETU LAAKSO,
VESA KUIKKA &
KIMMO K. KASKI

A Capability-Based Approach to Identifying and Remediating Cybersecurity Gaps in Critical Infrastructure

Cyber threats have grown rapidly worldwide, and healthcare remains one of the most frequently targeted critical infrastructure sectors¹, partly because its core mission is patient care rather than cybersecurity, and partly because sensitive patient data must remain continuously available. A wealth of high-quality guidance on cybersecurity best practices already exists, such as the ISO 27000 series and the NIST Cybersecurity Framework 2.0². These frameworks describe what an organization should do, but offer limited guidance on the order and emphasis in which measures should be implemented. This is a particularly important consideration for small and medium-sized enterprises, where resources are scarce³.

In this article, we present how a capability-based assessment model originally developed for the defense

sector⁴ can be adapted to support cybersecurity decision-making. We tested the model in a private healthcare organization that has no dedicated IT or cybersecurity unit, but which falls within the scope of Finnish national cybersecurity legislation derived from the EU- NIS2-Directive.

Method in a Nutshell

In the model, cybersecurity capability is divided into sub-capabilities, such as governance, access control, monitoring, and crisis communication. Each sub-capability is assigned a target level: what can reasonably be expected of the organization given its size, sector, and available resources. The difference between the current state and the target level is the capa-

bility gap. The larger the gap, the further the organization is from its target level.

Not all gaps are equally serious, however. Each sub-capability is therefore also assigned an importance weight, reflecting how severe the consequences would be if the gap were left unaddressed. Two equally sized gaps can therefore carry different weight in the outcome, depending on how critical the underlying issue is.

When an organization considers improvement measures, for example hiring additional staff, staff training, or a new governance model, the model calculates how much each measure reduces each identified gap relative to its overall input. This makes visible which measures deliver the most improvement relative to the effort invested, and allows

different improvement paths, such as a “high-impact” versus a “low-effort” approach, to be compared before resources are committed.

Use Case: A Healthcare Organization

We applied the model to a private healthcare organization that provides continuous care services across

multiple locations. The organization has no dedicated IT department; cybersecurity functions are largely outsourced, and responsibilities are shared under a “many hats” principle. Nevertheless, the organization is part of national critical infrastructure, and a significant number of people depend on the continuity of its services.

As input to the model, we used the organization’s existing IT risk

register, in which risks had already been classified as strategic, operational, or tactical. We interpreted each risk as an indicator of an underlying capability gap and mapped it to one or more sub-capabilities. Figure 1 illustrates the full workflow: from identifying risks, to assessing capabilities, defining measures, constructing scenarios, and finally comparing them before a decision is made.

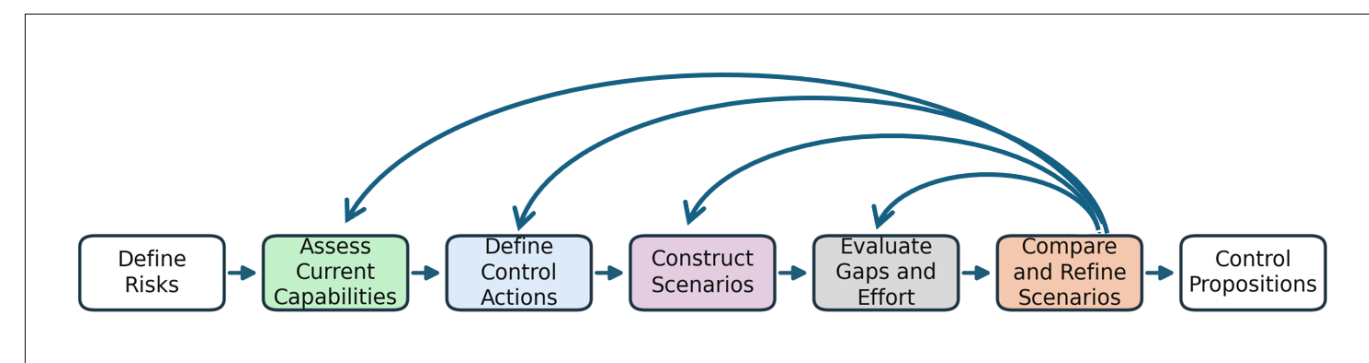


Figure 1. A capability-based workflow for improving cybersecurity: from defining risks to comparing scenarios and iteratively refining them before control decisions are made.

Results: Two Improvement Scenarios

We constructed two comparative improvement scenarios, in each of which three measures were selected for implementation within a limited planning period. Scenario 1 (“high impact”) prioritized measures expected to reduce the importance-weighted gaps the most: the selected measures were adequate staffing, crisis communication guidance and exercises, and the establishment of a cybersecurity governance model. Scenario 2 (“low effort”) prioritized measures with the lowest estimated implementation effort.

Scenario 1 reduced the remaining importance-weighted capability gap by roughly 13%, while Scenario 2 achieved a reduction of roughly 9%. The high-impact strategy thus produced a clearly larger relative improvement, but the low-effort

strategy also delivered meaningful benefit, which is an important finding for organizations that cannot afford to implement every costly measure at once.

Figure 2 shows how the gaps decreased across different risks under Scenario 1: the reduction was not uniform everywhere, with a particularly large improvement visible in the risk related to weak cybersecurity governance (Risk 1). This indicates that the selected measures were particularly well aligned with the sub-capabilities underlying that risk.

Conclusions

The results show that a capability-based model originally developed for military use is also applicable to supporting cybersecurity decision-making in a resource-constrained critical infrastructure organization. The model

does not provide an absolute measure of an organization’s security level; rather, it functions as a comparative decision-support tool: it helps reveal which measures deliver the greatest benefit relative to effort, makes the basis for prioritization transparent, and thereby makes it easier for decision-makers to commit to investment decisions.

It should be noted that this is a single case study, and that the transferability of the model from the defense sector to cybersecurity is, at this stage, an assumption rather than a rigorously proven result. The assessment of gaps and the effects of measures was also based on the judgment of a single expert. In future work, we intend to apply the model to more organizations and across different critical infrastructure sectors, and to involve multiple assessors to improve the model’s generalizability and reliability.

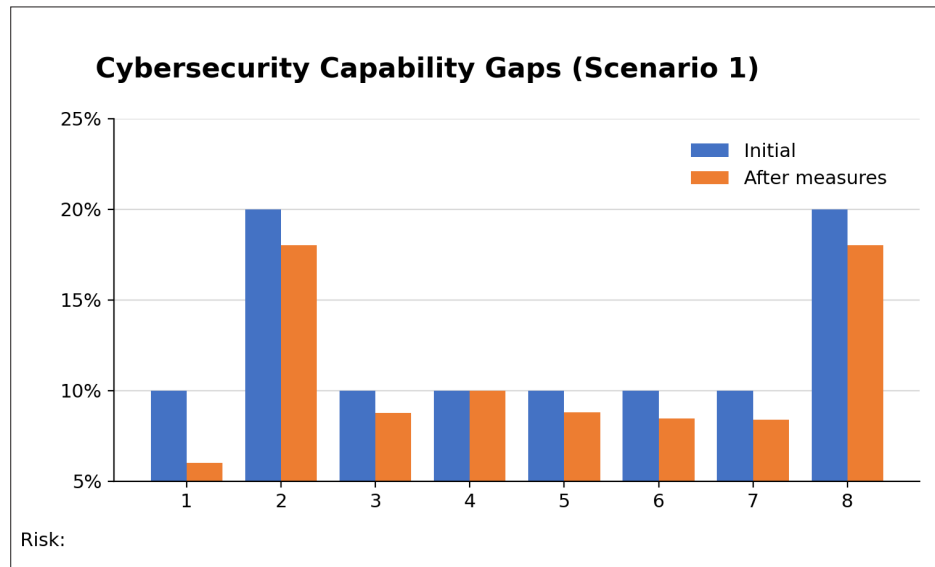


Figure 2. The effect of Scenario 1 on cybersecurity capability gaps by risk: the initial gap compared with the gap after the improvement measures. Risks: 1) weak cybersecurity governance, 2) reputational risk, 3) supply chain disruptions, 4) regulatory non-compliance, 5) inadequate data oversight, 6) lack of technical readiness, 7) data breach or manipulation, 8) post-incident reputational and regulatory impact.

REFERENCES/SOURCES

- 1 ENISA (2023) Health Threat Landscape Report. European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/publications/health-threat-landscape> (accessed 18 Jan 2026).
- 2 National Institute of Standards and Technology (2024) Cybersecurity Framework 2.0. NIST, Gaithersburg. Available at: <https://www.nist.gov/cyberframework> (accessed 27 Dec 2025).
- 3 El-Hajj, M. and Mirza, Z.A. (2024) "Protecting Small and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool", *Electronics*, 13(19), article 3910. doi:10.3390/electronics13193910
- 4 Kuikka, V. and Peltotalo, S. (2022) "A Method for Assessing Effects of Technological Development on Military Capabilities", *Proceedings of the International Conference on Decision Aid Sciences and Applications (DASA)*, IEEE, pp. 1634–1639.

AUTHORS:

EETU LAAKSO

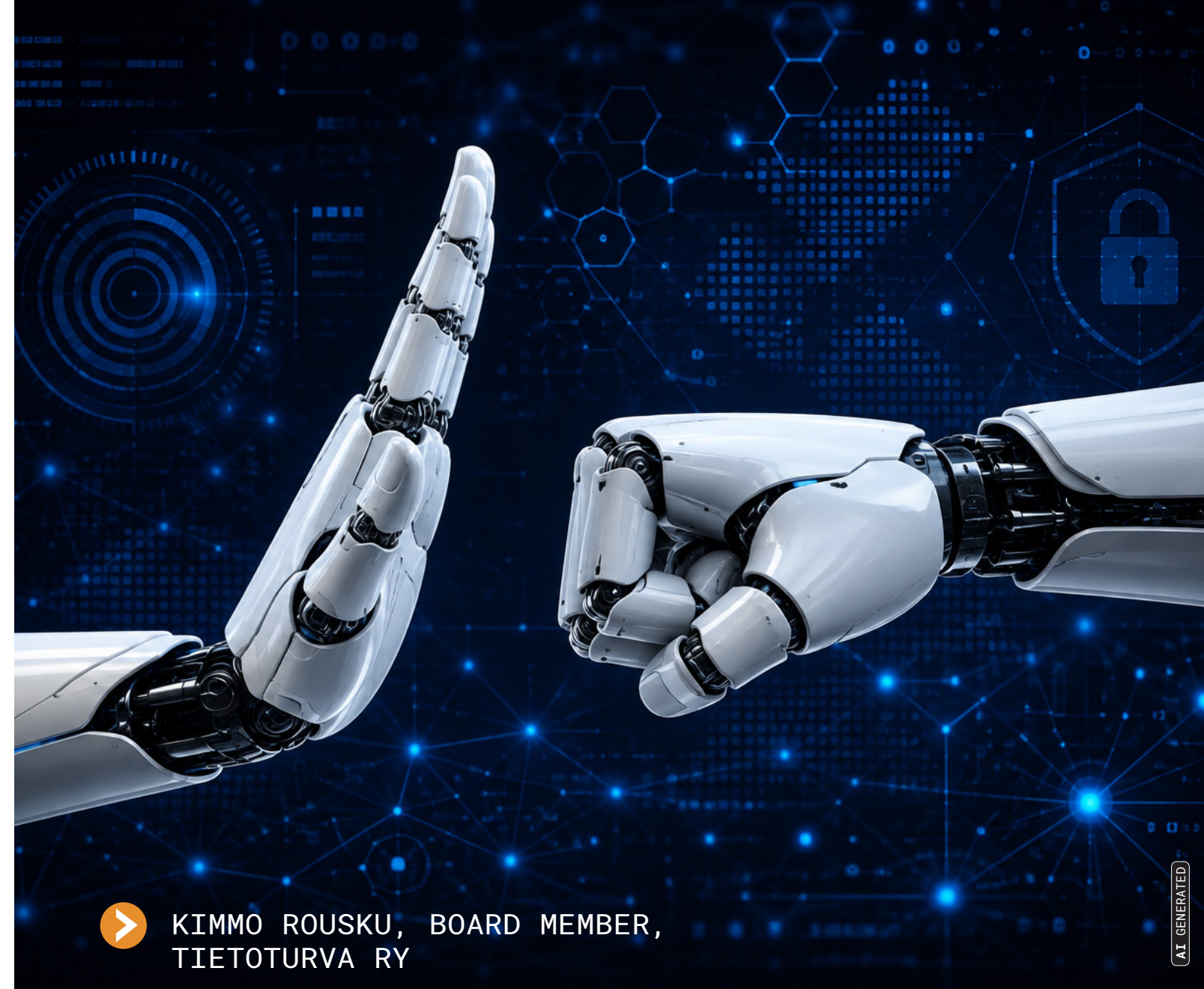
Eetu Laakso works at CyberWatch Finland in cybersecurity governance, risk, and compliance (GRC). He holds a B.Sc. in Pharmacy from the University of Helsinki and an M.Sc. in ICT and Cybersecurity from the University of Turku. This article is based on his first academic publication.

VESA KUIKKA

Vesa Kuikka holds a Doctor of Military Sciences degree from the National Defence University (2021) and a D.Sc. (Technology) degree from Aalto University (2022). His research addresses military capability modelling, stochastic combat and network-centric warfare, complex networks, cyber analysis, information diffusion, and resilience, integrating statistical physics, probabilistic modelling, and systems engineering.

KIMMO K. KASKI

Kimmo Kaski serves as an emeritus professor at the School of Science at Aalto University, and he is an internationally recognized Computational Science researcher. He specializes in the study of complex systems, including social and information networks, and utilizes data analytics of large datasets and computational modeling methods in his work.



Two Phenomena that Will Change Everything About Security

Artificial intelligence is transforming both attack and defence at the same time. Meanwhile, AI is uncovering so many software vulnerabilities that the old way of monitoring, assessing and deploying security updates is no longer sufficient. These two phenomena will not change cybersecurity alone. They will transform risk management, business continuity, preparedness, information security and data protection.

The score could be 112–13

Imagine a basketball game in which a human is playing against an adversary that uses AI effectively. The final score could be brutal: 112–13.

A human cannot monitor millions of events simultaneously, examine vast amounts of software code, compare findings against every known vulnerability or respond to every anomaly within seconds.

AI can do all of this continuously, around the clock and at tremendous speed – genuinely 24/7.

But the game is not lost!

When humans use AI as an ally, we can level the score. AI contributes speed, scale and the ability to process enormous volumes of data. Humans contribute an understanding of the operating environment, values, accountability, judgement and the ability to make decisions under uncertainty. These

human qualities can even help us win. That is why my advice is simple: **AI must be deployed across all areas of defence.** Not to remove humans from security work, but to strengthen our ability to see, understand, anticipate and act. If the attacker uses AI and the defender does not, it is not a fair contest.

The physics of vulnerability discovery has changed

The ability of AI models to discover software vulnerabilities has improved extremely rapidly. In February 2026, Anthropic reported that it had used its Claude model to discover and validate more than 500 serious vulnerabilities in open-source software.

Some of them had remained undetected for decades. The model did not merely search for familiar coding errors. It reasoned about how the software operated, examined previous fixes and found similar areas that had remained unpatched¹.

Microsoft, in turn, announced the deployment of MDASH, a system in which more than 100 specialised AI agents search for, assess, challenge and validate potential vulnerabilities. The May 2026 security updates included 16 vulnerabilities discovered by the system, four of which were critical remote code execution vulnerabilities.²

In July, Microsoft issued a direct warning that customers should prepare for larger volumes of security updates. According to the company, AI is finding more problems, more

quickly and across broader software environments³. OpenAI has described the change even more directly: vulnerability discovery used to be the bottleneck, but remediation is now becoming the new bottleneck⁴. This is an enormous change!

Update volumes reveal the direction of travel

The figures below are not fully comparable. Microsoft publishes monthly update packages, whereas Oracle uses both targeted monthly updates and extensive quarterly updates. Linux is not a single vendor but a broad ecosystem. Nevertheless, the table shows very clearly where we are heading.

TARGET AND CALCULATION METHOD	MAY 2026	JUNE 2026	JULY 2026
Microsoft Patch Tuesday	120 vulnerabilities, including 29 critical RCE vulnerabilities and no reported zero-days	200 vulnerabilities, including 33 critical vulnerabilities and six zero-days	570 vulnerabilities, including 59 critical vulnerabilities and three zero-days
Oracle	35 new fixes in the first targeted CSPU update	245 new fixes in a CSPU update	1,449 new fixes in the extensive quarterly CPU update
Linux ecosystem	1,706 vulnerabilities in the continuously updated Linux Patch Wednesday dataset; the first published summary included 1,638 vulnerabilities, 474 of them in the Linux kernel	1,888 vulnerabilities, including 324 in the Linux kernel	The month is still in progress; more than 400 Linux kernel CVEs were published on 19–20 July alone, within approximately 24 hours

Microsoft’s figures are based on its Patch Tuesday summaries for May⁵, June⁶ and July⁷. Oracle’s figures come from the company’s own announcements: May⁸, June⁹ and July¹⁰. In May, Oracle launched a

new series of targeted Critical Security Patch Updates to supplement its quarterly updates.

The Linux figures come from the independent Linux Patch Wednesday dataset¹¹, which com-

piles security advisories from different distributions. The July spike of more than 400 CVEs¹² concerned upstream Linux kernel disclosures, so it should not be compared directly with the previ-

ous months’ figures for the entire ecosystem.

What should we conclude from these figures?

The first **incorrect conclusion** would be that software has suddenly become dramatically worse. A more likely explanation is that we now have a much more powerful “microscope”. AI is discovering defects in both old and new software that humans, fuzzing tools and earlier code-analysis tools failed to detect.

The second incorrect conclusion would be that AI discovered every vulnerability listed in the table. It did not. The figures also include vulnerabilities identified using traditional methods, weaknesses in third-party components, variants of previously fixed vulnerabilities and peaks caused by update publication schedules. Nevertheless, the direction of travel is clear: **we will discover more vulnerabilities in the future, and we will discover them faster.**

Attackers benefit from the same technological advances. They can analyse a newly released patch, locate the modified code, infer the original vulnerability and produce a working exploit more quickly than before. Previously, an organisation might have had days or weeks to respond. In the future, it may have only hours – and soon, perhaps only minutes.

Vulnerability management is no longer a monthly maintenance task

Many organisations still treat security updates as a technical and almost mechanical maintenance task: updates are reviewed on a specific day, tested, moved to the next maintenance window and finally reported. This operating model will simply be too slow in the future. Vulnerability management must become a continuous, risk-based process.

An organisation must know:

1. What devices, services, applications, interfaces, cloud environments and software components does it have?
2. Where are they used, and are they connected to the internet?
3. What data and functions can be accessed through them?
4. Is working exploit code available for the vulnerability, or is there evidence of active exploitation?
5. What temporary protective measures can be implemented before a permanent fix is available?
6. Who is authorised to restrict or shut down a service? This capability must be available 24/7, regardless of whether senior management can be reached.

A CVSS score alone is no longer sufficient. Prioritisation also requires information about the criticality of the service, its actual exposure, the likelihood of attack, the availability of exploitation methods and the potential scale of the damage. AI is needed to combine and analyse these volumes of information. Humans are needed to decide which risks the organisation can accept.

Sometimes the safest option is to shut down a service – for a while!

If an internet-facing service has a serious or critical vulnerability, no patch is available and attacks are already being observed elsewhere in the world, keeping the service operating normally may be significantly more dangerous than temporarily restricting or shutting it down. Shut-down must not become an automatic response to every vulnerability. An outage can also endanger operational continuity, safety, human health or the availability of critical, statutory services.

The decision must be made by comparing two risks:

1. **What happens if the service is shut down?**
2. **What happens if the service is compromised?**

A temporary and controlled outage may sometimes be the best way to protect continuity. A controlled outage may last only a few hours. Investigating a serious breach, rebuilding systems, restoring data, notifying customers and repairing lost trust can take months and cost millions of euros.

If no patch is available, possible measures may include disconnecting the service from the internet, disabling the vulnerable function, blocking a protocol or specific traffic, restricting access rights, segmenting the network, deploying WAF or IPS protection, and increasing logging and monitoring. These measures must, however, be planned in advance. A crisis is the wrong time to determine for the first time who is authorised to shut down the organisation’s critical service.

What will be the outcome? The number of data breaches will increase

It is virtually certain that AI will increase the number of attempted attacks. AI reduces costs, automates reconnaissance, searches for weaknesses, adapts attacks to their targets and makes it possible to chain multiple vulnerabilities together.

It is also highly likely that the number of successful data breaches will increase, at least over the next few years. Not all organisations can update their systems quickly enough. Some do not even know where a vulnerable component is being used. Particularly high risks are associated with legacy systems, customised applications, industrial environments, supply chains and software that is no longer supported by its vendor.

Data breaches rarely result from a single mistake. AI is particularly effective at discovering attack chains: a minor data leak can be combined with weak authentication, a misconfiguration, excessive access rights and, ultimately, an exploitable vulnerability. Attackers do not need to break through an organisation's strongest point. They only need AI to find the weakest link. If that link is not inside your organisation, AI can map the supply chain formed by the services and suppliers you use and search for the weakest link there.

New software can be made more secure than before

Fortunately, this development also has a highly positive side. If AI can search for vulnerabilities in finished software, it can also be used before the software is released. AI can review code, analyse architecture, create threat models, identify dangerous dependencies, generate test cases and search for different ways to compromise an application.

The objective cannot be software that is completely resistant to AI-assisted attacks. After all, perfect, 100 % security does not exist. We can, however, build software that is significantly harder for an AI-assisted attacker to compromise. This requires security to be incorporated from the design stage onwards:

1. Secure default settings and the smallest possible attack surface.
2. The principle of least privilege, strong authentication and the separation of functions.
3. The use of memory-safe programming languages whenever appropriate.
4. Visibility into software components and dependencies through software bills of materials, or SBOMs.
5. Continuous AI-assisted review of code, interfaces and changes.
6. Logging, monitoring and the ability to detect even a successful attack.
7. The ability to update a vulnerable function or, when necessary, disable it quickly.
8. Human review of critical findings, fixes and decisions.

AI must therefore be present on both the red team and the blue team: attempting to break the system before criminals do, and helping defenders fix the weaknesses it discovers.

The change extends across all areas of digital security

Risk Management

A traditional risk register can become outdated before the next meeting even takes place. AI can continuously monitor threat intelligence, vulnerabilities, asset information, supply chains and changes in the operating environment. It can develop new risk scenarios, identify dependencies and assess how a disruption affecting one supplier or component could impact other services. Humans must still determine the significance and acceptability of a risk and decide what actions are required. AI must not be allowed to decide on its own what level of risk to people, society or an organisation is acceptable.

Business continuity and preparedness

AI can help identify critical dependencies, simulate disruptions, design exercises and update operating instructions based on lessons learned. It can also support incident management by rapidly building situational awareness, assessing alternatives and identifying the potential consequences of decisions. At the same time, organisations must prepare for disruptions to AI services themselves, inaccurate responses, manipulated input data and situations in which an important service is unavailable. AI also requires a continuity plan and an alternative operating model.

Information Security

AI is needed to discover vulnerabilities, map attack surfaces, analyse logs, detect anomalies, combat phishing, examine malware and prioritise events. The role of a security operations centre is no longer merely to detect individual alerts. With the help of AI, it must be capable of identifying rapidly evolving attack chains. At the same time, AI systems create a new attack surface. Models, agents, tools, extensions, inputs, memories, access rights and the data they process must be protected in the same way as other critical systems.

Data Protection

AI can help identify personal data, maintain records of processing activities, assess data protection impacts, monitor retention periods and detect abnormal uses of data. However, AI can also infer highly sensitive information from seemingly harmless data. It can combine fragmented information, re-identify individuals in anonymised datasets or distribute personal data uncontrollably between agents and integrations.

One issue that particularly concerns is the increasingly sophisticated profiling of us as individuals.

In the future, data protection cannot focus solely on what information is stored in a system. We must also ask what AI can infer from that information, to whom it can disclose the information and what actions it can initiate.

What must organisations do now?

The first step is not to “go shopping” for a new AI service. The first step is to identify where humans working in security are already losing in terms of speed, scale or detection capability.

The organisation must then:

1. Build and maintain an up-to-date inventory of devices, services, software and dependencies.
2. Deploy AI in the analysis of vulnerabilities, threats and anomalies.
3. Move from a monthly update cycle to continuous, risk-based vulnerability management.
4. Define remediation deadlines for different risk levels and monitor compliance with them.
5. Agree in advance when a vulnerable service should be restricted or shut down.
6. Exercise a scenario in which no patch is available for a critical service.
7. Use AI for threat modelling, testing and code review when developing new software.
8. Keep humans accountable for critical decisions and for the quality of AI-generated findings.

AI will not eliminate the need for security professionals. On the contrary, it will increase the need for skilled people because there will be more findings, fixes and decisions than ever before. Security still does not come from technology. It comes from people. But in the future, security can no longer be built without AI.

REFERENCES/SOURCES

- 1 Anthropic: Evaluating and mitigating the growing risk of LLM-discovered 0-days: <https://www.anthropic.com/research/zero-days>
- 2 Microsoft: Defense at AI speed: <https://www.microsoft.com/en-us/security/blog/2026/05/12/defense-at-ai-speed-microsofts-new-multi-model-agentic-security-system-tops-leading-industry-benchmark/>
- 3 Microsoft: Evolving Windows vulnerability management: <https://blogs.windows.com/windowsexperience/2026/07/09/evolving-windows-vulnerability-management-to-meet-the-speed-of-ai-powered-discovery/>
- 4 OpenAI: Daybreak: <https://openai.com/index/daybreak-securing-the-world/>
- 5 <https://cybersecuritynews.com/microsoft-patch-tuesday-may-2026/>
- 6 <https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2026-patch-tuesday-fixes-6-zero-days-200-flaws/>
- 7 <https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2026-patch-tuesday-fixes-massive-570-flaws-3-zero-days/>
- 8 <https://www.oracle.com/security-alerts/cspumay2026.html>
- 9 <https://www.oracle.com/security-alerts/cspujun2026.html>
- 10 <https://www.oracle.com/security-alerts/cpujul2026.html>
- 11 <https://github.com/leonov-av/linux-patch-wednesday>
- 12 <https://cybersecuritynews.com/linux-patches-400-kernel-vulnerabilities/>

AUTHOR:



KIMMO ROUSKU
Tietoturva ry,
Board Member





➤ RISTO RAJALA
& PETER SUND

The Importance of Resilience and Reliability is Becoming Even More Pronounced as Cybersecurity Transformation Trends Intensify

The accelerating development of the most advanced AI models and their impact on cybersecurity have sparked intense debate, as some models have reportedly found tens of thousands of vulnerabilities in critical software. With the spread of even simpler AI tools, the average time between dis-

covering a vulnerability and exploiting it has shortened significantly, in practice from days to even hours. Despite the development and wider use of AI models, the fundamentals of cybersecurity have not changed and are not changing. The importance of everyday digital risk man-

agement is increasing further. This includes maintaining inventories of devices and software, systematic vulnerability management and patching, identity and access management, network segmentation, continuous monitoring, and log analysis. Preparing for the cybersecurity impact

of AI software is therefore primarily about the speed, automation, and scaling of corrective measures.

The most advanced AI models currently available have been developed and are administered outside Finland and the European Union. This, together with other concerns about the availability and continuity of critical digital services, has strongly influenced the political debate in Europe and increased demands to strengthen digital sovereignty. From a cybersecurity perspective, it is clearly problematic if European organisations have only very limited, or no, access to the most advanced AI models. The erratic, unpredictable, and at times hostile policy direction of the United States has added fuel to the fire. The June decision to limit access to Anthropic's Claude Fable 5 model to US citizens only, after it had briefly been available globally, showed plainly the EU's vulnerable position and its dependence on the diminishing goodwill of the US administration. Although the restriction was later lifted, the United States has now demonstrated that it has both the will and the ability to restrict access in the EU to digital services provided by companies under its jurisdiction.

The debate on strengthening the EU's digital sovereignty has continued intensely. The Union's lack of leverage in the face of unilateral US export restrictions has shocked many policymakers. Although concerns about access to the most advanced AI models have dominated public debate, it is important to note the broader picture: more than 80% of the digital products, services, and infrastructure used in the EU come from outside the Union. In addition, European companies spend EUR 264 billion and the public sector at least an estimated EUR 50 billion each year on purchases mainly from US IT suppliers. The direction of EU technology policy is therefore moving strongly towards reducing the most

critical dependencies and favoring European technologies in the name of sovereignty. Finnish Information Security Cluster (FISC) nevertheless speaks of digital sovereignty through the lens of strategic autonomy, because we consider the term "sovereignty" problematic in this context. Achieving a state comparable to national sovereignty is neither realistic nor desirable in a networked digital world. Strategic autonomy, where dependencies are managed, better describes a balanced target state. FISC particularly emphasises the importance of ensuring the continuity and resilience of digital services and the reliability of actors in supply chains.

The EU technology sovereignty package

The EU technology sovereignty package was published in June 2026. It includes the Cloud and AI Development Act (CADA), the new Chips Act 2.0, the open-source strategy, and a roadmap on the role of AI and digitalisation in the energy sector. The common objective of the package is to reduce critical dependencies on technologies from outside the EU and to strengthen Europe's competitiveness, resilience, and strategic autonomy. From the perspective of the cybersecurity industry, CADA is the most important part of the package, although the strategic management of open-source activities should not be underestimated. CADA aims to increase Europe's cloud and AI capacity, create a sovereignty framework for cloud services, introduce new public-sector procurement obligations, and establish a EuroCloud federation and joint procurement framework. The proposal is broadly heading in the right direction, as it seeks to build strategic autonomy primarily through competitiveness, investment, and European expertise. Regulatory requirements must, however, be clearly defined and risk based.

CADA's sovereignty framework would guide public-sector cloud procurement through four "trust levels". At the lowest level, data processing within the EU and self-assessment would be sufficient, while the higher levels would include stricter requirements concerning, for example, third-country influence, ownership, supply-chain transparency, and audits. This risk-based model is preferable to rigid one-size-fits-all sovereignty requirements. For SMEs, it is important that recognition once granted is valid across the EU without separate national approvals. However, the key market-access criteria should be written into the regulation itself and should not be substantially changed through delegated acts without sufficient transition periods. The biggest practical risk is that trust levels 2–4 rely on the EU cloud services cybersecurity certification scheme, EUCS, which has not yet been finalised. If EUCS is delayed, temporary national solutions could fragment the EU internal market. From Finland's perspective, it is important that national assessment practices, such as KriPa for cloud services, are recognised during the transition period. A clear deadline should be set for EUCS before procurement obligations for the higher levels enter into force. Certificates and audits should also be accepted as evidence of compliance with NIS2 and CRA requirements, so that companies do not face overlapping obligations.

The recognition and audit procedure proposed in CADA should be streamlined. National assessment, consultation of Member States, possible objections, and a Commission decision could together make the process slow and difficult to predict. This would be particularly problematic for SMEs and fast-developing services. A binding overall deadline is therefore needed for the procedure. Audit capacity must also be built in time so that annual audits do not become a bottleneck. In Finland, the National Cyber Security Centre

within Traficom is likely to be designated as the competent authority, which will probably require additional allocation of authority resources, possibly by giving up some other tasks. At the same time, it must be ensured that the sanctions framework is consistent at EU level. Proportionality must also be ensured in procurement obligations. Taking multi-vendor and multicloud strategies into account is positive, but the Commission should not be able to override a Member State's own risk assessment in matters related to national security. A 12-month transition period for mandatory cloud migration may also be unrealistic for large public-sector systems. Such a broad market intervention must be based on the genuine availability of recognised services, and the grounds

for exceptions must be clear. It must also be ensured that CADA does not create overlaps with NIS2, the CRA, KriPa, or the Act on Information Management in Public Administration.

CADA can open up new business opportunities in cloud and AI services, assessment and audit services, cybersecurity testing environments, critical infrastructure services, and joint procurement. In particular, the objective of directing part of procurement towards innovative SMEs is positive, provided that the related reporting and other administrative requirements remain light. At the same time, procurement criteria related to European added value must be handled carefully: they must not discriminate against Finnish export compa-

nies operating in global value chains, and WTO obligations must also be taken into account.

The proposed EuroCloud federation could improve the use of public-sector capacity, but it must not distort the market. Public authorities should not provide services that the market can offer. Capacity sharing should be limited to the use of genuine surplus capacity, and the same security and trust-level requirements should also apply to shared services. Supporting open source is advisable only if security, maintenance, and lifecycle responsibilities are properly managed. The proposed recognition mechanism for third countries is an important flexibility tool, as it enables effective cooperation with trusted partner countries. The criteria must, however, remain clear,

and transition periods must be provided for any withdrawals. Overall, CADA can strengthen the European cloud and AI market if it is implemented in a predictable, risk-based way that supports companies' competitiveness.

Cybersecurity and AI roadmap

Soon after the sovereignty package, the Commission published its cybersecurity and AI roadmap in July 2026. This is a non-legislative plan for how the EU will respond to the cybersecurity risks caused by AI and use its opportunities to strengthen cybersecurity. The roadmap aims to make advanced AI safely accessible for cybersecurity use, prepare Euro-

pean organisations for AI-enhanced threats, and scale European AI-based cyber solutions.

The roadmap sets out the creation of an evaluation mechanism for AI models within the Commission's AI Office. One purpose would be to assess the cybersecurity impacts of AI models before they enter the market. According to the roadmap, the Commission and the European Union Agency for Cybersecurity, ENISA, will also prepare by the end of 2026 a structured plan under which European authorities, critical infrastructure operators, cybersecurity companies, and researchers could gain structured access to the most advanced AI models. It remains unclear, however, how companies administering the most advanced AI models from third countries will respond to these proposals, or whether they are interested in cooperation at all. ENISA and the Commission's Joint Research Centre will also prepare a testing platform where companies and research institutes can test AI-based cybersecurity solutions in controlled environments before deployment. This could create business opportunities for companies operating cyber ranges and assessment bodies.

The second part of the roadmap concerns preparedness. ENISA is expected to publish guidance on protecting against AI-enhanced threats and on the safe use of AI in cybersecurity operations. At the same time, the roadmap sets out the need to update coordinated vulnerability disclosure practices in cooperation between EU institutions, Member States, and industry, because AI may increase the number of automated and low-quality vulnerability reports. The EU will also launch a critical open-source resilience campaign to identify important open-source components and support their maintenance and security.

The third part concerns investment and skills. Through the European Cybersecurity Competence Centre, the EU plans to launch a

Grand Challenge on AI-assisted vulnerability remediation at the end of 2026, and to make use of AI factories, computing capacity, training modules, and an updated cybersecurity skills framework. The exact form and content of the challenge remain unclear, but it will certainly offer funding and business opportunities for the Finnish cybersecurity industry.

The importance of trusted suppliers is increasing

In light of recent events, the public debate on sovereignty and strategic autonomy has understandably focused on the availability and continuity of digital services provided by companies operating under the jurisdiction of countries outside the EU. The share of third-party risk in cybersecurity incidents is constantly growing, and the weakest link in the supply chain accounts for an increasing share of overall risk. From a cybersecurity perspective, it is essential also to pay attention to the reliability and possible risks of software and components produced from outside the EU and included in supply chains. A low price may be based on weak quality control or, in the worst case, even an intentional software vulnerability that is not detected in ordinary inspections — not to mention hidden and unlawful data flows. Low-cost suppliers often avoid or fail independent security audits, leaving vulnerabilities and the origin of components unverified. Low prices may also be achieved through long and opaque subcontracting chains, meaning that the final buyer does not know who actually manufactured or coded the components.

Some supply-chain risks may be directly linked to the supplier company's home country, for example because of its legislation, political system, or operating practices. Companies operating from authoritarian countries may be legally obliged to



hand over data or access rights to state authorities without the customer being informed. Devices and software also require continuous updates from the manufacturer, and if the supplier is under the influence of an authoritarian third country, the update channel itself may become a possible attack route. At the geopolitical level, dependence of critical infrastructure on a single authoritarian state gives that state the ability to use the supply chain as leverage in a crisis, for example by cutting deliveries or exploiting remote access.

Significant measures to mitigate supply-chain risks are currently being prepared in the EU legislative process. Although they are not formally part of the Commission's sovereignty package, their practical impact may be even greater than the measures presented in June. In spring 2026, the Commission presented a legislative proposal for a comprehensive reform of the Cybersecurity Act. The aim of the proposal is to create a stronger and more coherent EU cybersecurity system by reforming ENISA's powers and modernising and expanding the cybersecurity certification system. The most significant part of the proposal is the creation of an EU-level mechanism for managing ICT supply-chain risks. This would be based on an EU-level, risk-based, and technology-neutral framework aimed at identifying critical ICT components and related supplier dependencies and assessing associated non-technical cyber risks such as third-country legal or geopolitical influence. Although the previously adopted NIS2 Directive and, in particular, the Cyber Resilience Act also address supply-chain risks, the mechanism as proposed would fill a gap that those two instruments cannot cover. The Commission's proposal for a Digital Networks Act will also affect the overall picture. Its objectives of strengthening the security, resilience, and robustness of digital networks are positive for business digitalisation and

European competitiveness, but it is important to ensure that the security-related provisions support investment and innovation and do not increase uncertainty or overlapping obligations in an already heavily regulated, risk-based operating environment. At the same time, the provisions must be fully compatible with other EU cybersecurity regulations.

Europe's cybersecurity depends on the success of industry

Ensuring cybersecurity is essential for the functioning of companies, organisations, and entire societies, and its importance will continue to grow. The development and spread of AI models highlight the need for speed and scalability in cybersecurity measures, but at its core the issue remains everyday digital risk management. In a situation where speed is decisive, it is even more impor-

tant that companies and organisations have a sufficient baseline level of cybersecurity that is automated where appropriate, especially when it concerns functions that are critical for society. At present, we estimate that in the sectors covered by the Cybersecurity Act alone there is an investment gap of up to more than one billion euros compared with the level required by law. It is therefore important that political decision-making also creates economic incentives for cybersecurity investments, for example by implementing a multiannual cybersecurity support programme during the next parliamentary term.

A strong and competitive cybersecurity industry is a prerequisite for the uplift in cybersecurity required by the development of AI, both in Finland and across Europe. Finnish Information Security Cluster actively works to safeguard the operating conditions of the cybersecurity industry in Finland and to increase its business opportunities.

AUTHORS:



PETER SUND

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



RISTO RAJALA

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



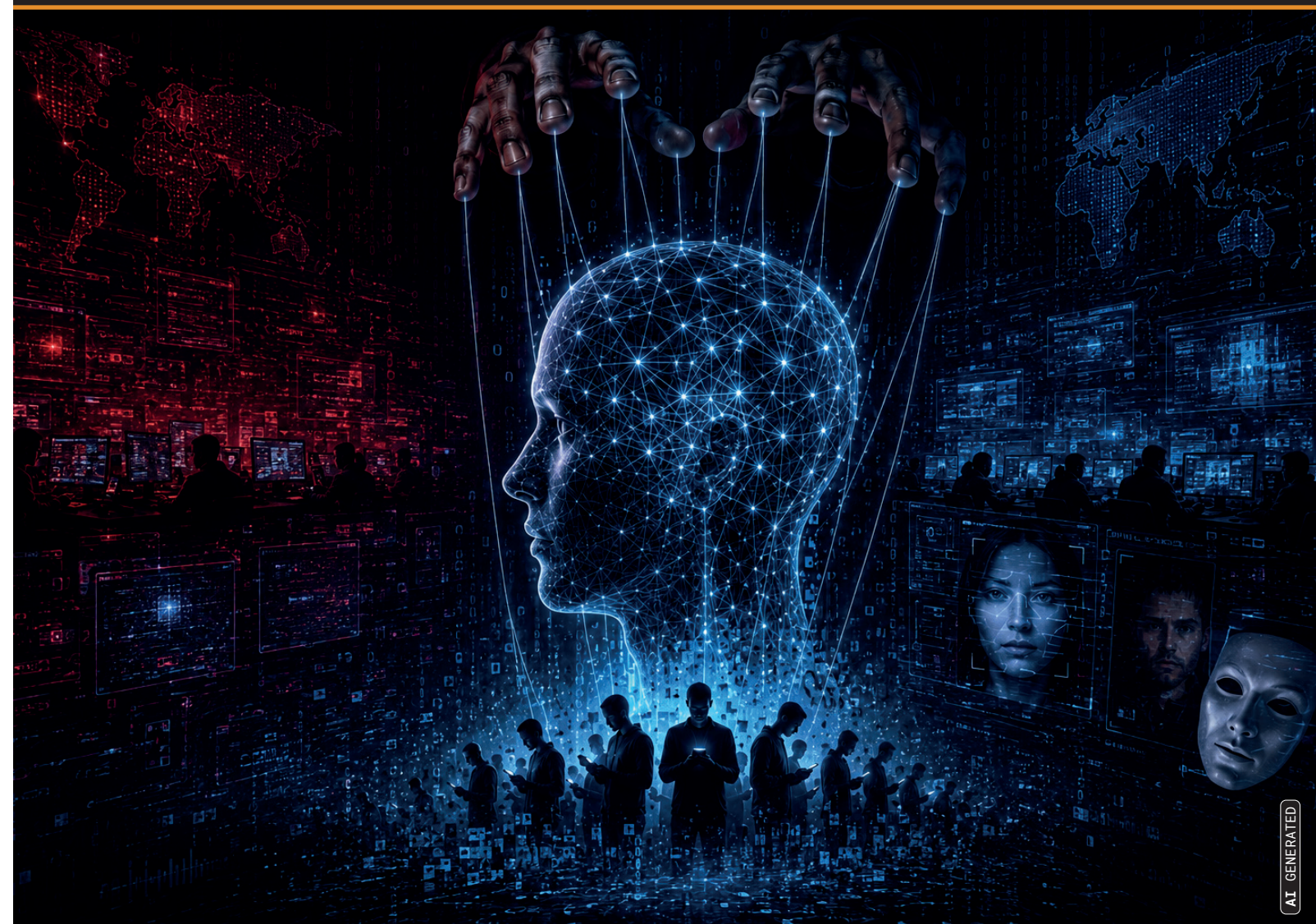
Cyberwatch Finland

WEEKLY REVIEW

29/2026

Themed Review

THE PSYCHOLOGICAL DIMENSION OF CYBERATTACKS AND CYBER-PSYCHOLOGICAL WARFARE



AI GENERATED





Introduction

An often-overlooked aspect of cyberattacks is the psychological impact they have on their targets. Although public attention tends to focus on stolen data, disabled systems, and financial loss, a growing body of research suggests that the most important dimension of many cyberattacks is quite often the psychological one. This is especially true of cyberat-

tacks carried out during active conflicts, as the recent wars in Ukraine and the Middle East have made clear. This summary sets out what cyber-psychological warfare is and how it fits within the broader concept of cognitive warfare, before examining how it has been used in practice in Ukraine and in the conflicts involving Iran and Israel.



What is Cyber-Psychological Warfare?

Cyber-psychological warfare is best understood as a sub-category of cognitive warfare — the branch of conflict concerned with shaping the mindset of the enemy. The two share the same fundamental objective, which is why it is reasonable to treat the former as a species of the latter. It is important, however, not to collapse the distinction entirely. Cognitive warfare is a considerably broader concept that also operates through non-cyber channels, including traditional propaganda, broadcast media, and face-to-face influence, whereas cyber-psychological warfare refers specifically to the pursuit of those cognitive effects through cyber means. It is therefore one instrument within the cognitive-warfare toolkit, not a synonym for it.

With an ordinary cyberattack, the psychological toll is a side effect of an operation aimed at some other end; in a cognitive operation, that same toll is the point. That said, the line is not rigid: even operations originally focused on physical disruption or destruc-

tion can turn out to be far more consequential psychologically than materially.

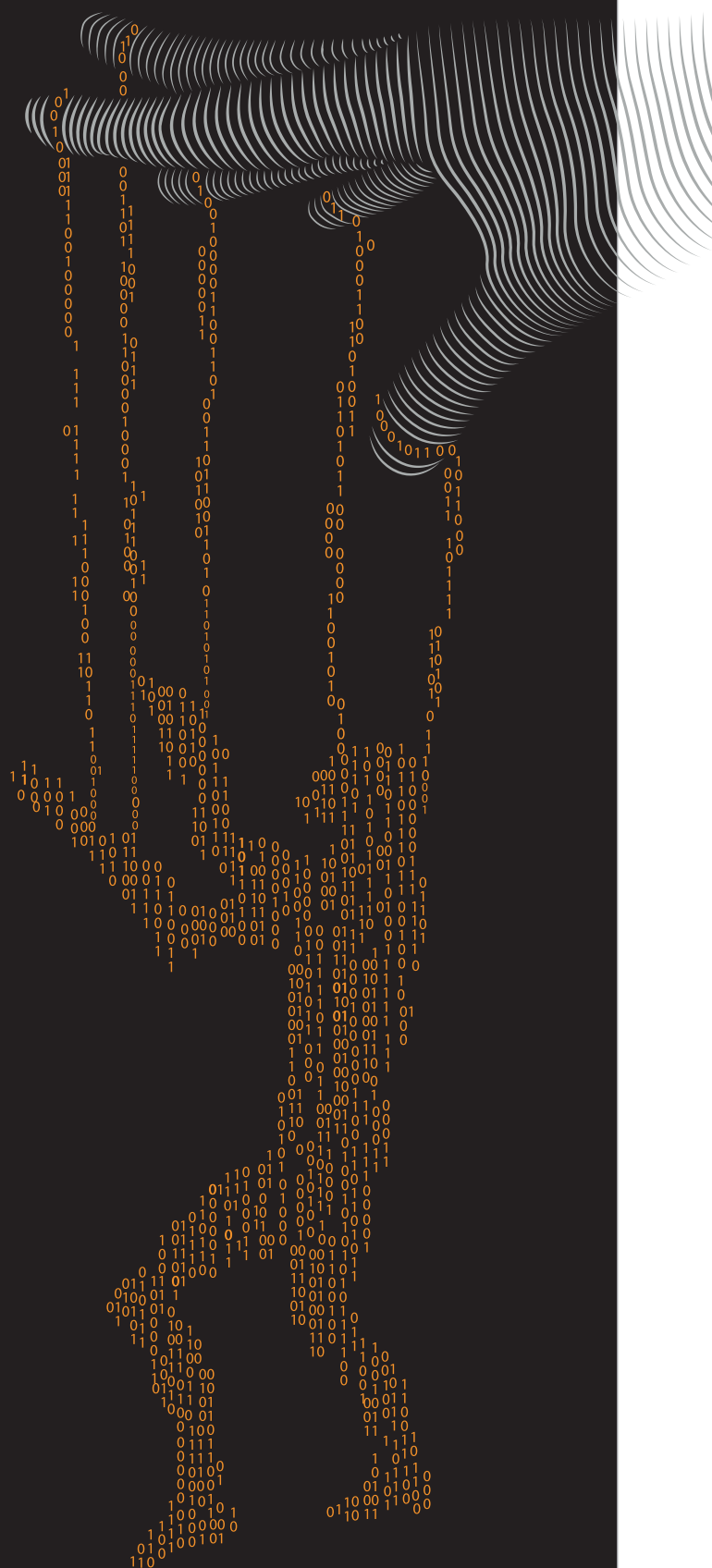
The psychological effects themselves are well documented at several levels. For individuals directly hit by a breach, ransomware, or fraud, research consistently describes an initial shock followed by a sense of vulnerability and violation, alongside anxiety, anger, and helplessness, and an ongoing fear of identity theft, financial fraud, or blackmail. In more severe cases the trauma is lasting, with clinicians reporting depression, anxiety, panic attacks, post-traumatic stress, and, in extreme cases, suicide, frequently accompanied by disrupted sleep and eating. Some researchers explicitly equate the experience of data-breach victims with that of trauma survivors. A recurring theme is the erosion of trust, as victims find it hard to trust organisations with their data afterwards, which can lead to isolation. Perhaps the most famous case in Finland is the Vastaamo breach which saw the information of over

30,000 patients and staff leaked. There has been psychological research on the subject, which can provide more information for those interested in the experiences of the victims.

The toll inside a targeted organisation is also heavier than the usual financial-and-reputational framing suggests. During an incident, anxiety spikes, decision-making becomes harder under pressure, and staff work punishing hours, producing both a psychological and a physical toll. Employees who inadvertently trigger a breach tend to carry guilt, shame, and fear, which feeds into lower morale and retention, and the strain on incident responders is particularly acute — one survey found that around 65% of them had sought mental-health assistance as a result of responding to cybersecurity incidents.

At the level of entire populations, experimental research shows that cyberattacks reliably evoke dread, anxiety, anger, and heightened threat and risk perceptions. Strikingly, exposure to cyberterrorism can generate negative emotions and threat perceptions at levels equivalent to those produced by conventional terror attacks; in one experiment, raised cortisol was used to demonstrate that people who experience higher stress after such an attack are more likely to support hardline retaliatory policies. The downstream political consequences are what make this strategically significant: distress drives diminished trust in government and heightened support for intrusive state surveillance at the expense of civil liberties, and widespread public distress can generate pressure for military retaliation, even across domains, cutting against norms of cyber de-escalation.

These findings also explain the cognitive-operations playbook. Ransomware crews, for instance, deliberately amplify fear by naming the specific audiences who might find out — regulators, competitors, the media — triggering compliance and breach-notification anxiety, and isolating individual administrators by threatening to contact their superiors. Scaled up to the level of the state, the same logic produces the core method: an intrusion on a hospital, a power grid, or an election system does limited physical damage but signals capability, manufactures a pervasive sense of insecurity, and corrodes confidence in the institutions people rely on. The measurable psychological reactions catalogued above — fear, distrust, demands for hard-line responses, and polarisation — are precisely the effects a cognitive operator sets out to produce.



Ukraine: Fear as a Weapon, Resilience as a Shield

The war in Ukraine is the clearest real-world case study available, and the pattern that emerges is telling: cyberattacks there have delivered relatively little military or physical effect while functioning largely as instruments of psychological and cognitive pressure. This framing recurs throughout the analytical literature; a 2023 analysis by Eyal Pinko for the Begin-Sadat Center for Strategic Studies (BESA) concluded that during the first year of the war the cyber domain had a negligible military effect and that the adversaries used cyber operations primarily for psychological warfare and to influence local and global public opinion.

The strongest single example is the December 2023 attack on Kyivstar, Ukraine's largest telecommunications provider. The operation disrupted mobile and internet services nationwide for around 24 million subscribers and knocked out air-raid warning systems in the Kyiv and Sumy regions. The head of the Security Service of Ukraine's cyber department said its objectives were to inflict a psychological blow to the public and to gather intelligence and framed it as a message and a warning — not only to Ukraine but to the wider Western world — that no one is truly untouchable. Disabling the air-raid alerts is the detail that turns disruption into terror, because it degrades the very system people depend on to feel safe during and in between strikes. CrowdStrike's assessment placed the incident in the same category, identifying an overarching motivation to contribute to psychological operations that seek to degrade, delegitimise, or otherwise influence public trust in state institutions and in sectors such as government, energy, transport, and media.

The wider record fits this reading. Chatham House's study of Russian cyber and information warfare found that cyberattacks not tied to any immediate tactical aim appeared designed to intimidate and demoralise Ukrainian defenders and documented deliberate

coordination with kinetic strikes: the autumn 2022 campaign against Ukrainian energy infrastructure showed operational-level coordination of disruptive cyber capabilities with missile strikes to maximise both physical and psychological impact. The various wiper-malware campaigns — such as WhisperGate, HermeticWiper and CaddyWiper — belong here too, since their value lies as much in signalling capability and manufacturing insecurity as in the data they destroy.

There is also a more targeted, personal strand: hacktivist groups such as Solntsepek have concentrated on deanonymising Ukrainian soldiers and publishing their personal data, a direct form of psychological pressure aimed at individuals and their families. The analysis by Miguel Alberto Gomez and Ryan Shandler for the Council on Foreign Relations argues that cyberattacks in the war have played a major role in degrading trust in societal institutions even while failing to produce significant physical effects — and degrading institutional trust is precisely the lever through which one would hope to erode war support.

The most important nuance, however, is that the evidence for any such erosion points the other way. Ukrainian resilience appears to have blunted the intended effect. Multiple assessments conclude that the Russian cyber campaign failed at the strategic level, with one arguing that it failed primarily because of Ukraine's effective cyber resilience rather than merely robust defences. At the level of sentiment,

Ukrainian society has largely held firm: well into the war, a majority still oppose territorial or political concessions to Russia, even as war fatigue grows. The dynamic also runs in both directions — Ukraine's volunteer IT Army and its highly visible campaigns are assessed to have bolstered domestic morale and projected national resilience to both domestic and international audiences.





Iran and Israel: The Shadow War for the Mind

The conflicts involving Iran and Israel arguably provide an even clearer illustration than Ukraine, because so many of the operations are explicitly built around a message rather than merely an effect.

On the Israeli-linked side, the central actor is Predatory Sparrow, known in Farsi as Gonjeshke Darande — a group widely believed by analysts and Israeli media to be tied to Israeli military intelligence, although Israel has never confirmed this and the group presents itself as Iranian anti-government hackers. Its operations are consistently marked by substantial disruption, deliberate data destruction, and provocative public messaging aimed at taunting the target. In a 2021 railway attack the malware disabled operations while displaying taunting messages across station boards; the 2021 fuel attack that disabled around 80% of Iran's petrol stations also saw the attackers take over digital billboards to display messages critical of the Supreme Leader; and after a 2022 steel-mill attack

that caused a fire, the group deliberately released footage of the damage.

The point of hijacking billboards and releasing footage is audience, not sabotage. During the June 2025 Twelve-Day War this escalated into the financial system: the group wiped data at the state-owned Bank Sepah and then struck the Nobitex exchange, destroying roughly \$90 million in cryptocurrency by sending it to inaccessible addresses and publishing the exchange's entire source code, using a wallet address containing an expletive aimed at the IRGC. Iranian state television was also hijacked to broadcast footage calling for a public uprising. Analysts describe the group's method explicitly as blending malware, precise timing, and psychological manipulation to erode an adversary's confidence.

The Twelve-Day War was where cyber and kinetic operations became fully braided. An analysis by the cybersecurity firm ZENDATA recorded that cyber-

»

attacks surged by around 700% within 48 hours, that more than 100 pro-Iranian hacktivist groups mobilised on Telegram, and that several pro-regime Iranian news agencies were compromised simultaneously in the opening hours of the strikes.

Iran's own approach leans far more heavily on fear and fabrication than on physical damage, partly to compensate for its conventional military disadvantage. The Foundation for Defense of Democracies labels the core tactic "perception hacking" — conduct designed to incite fear and influence opinion, often by exaggerating or entirely inventing the effects of an attack. The clearest illustration is the Handala group's dispatch of threatening texts to tens of thousands of Israelis claiming to have breached the Iron Dome and warning that they had seconds to escape; in reality the group had merely compromised a text-messaging system to stoke panic. On another occasion an Iranian persona claimed to have ransomed cameras at Nevatim Air Force Base, when the leaked footage actually came from a town that simply had a street of the same name.

Microsoft has documented how Iran wraps such operations in retaliation narratives and increasingly relies on bulk texts and emails, because a message arriving in someone's inbox or on their phone lands harder than one seen on social media. By 2025–2026 this had become more menacing and better synchronised, with Israelis fleeing missile strikes receiving texts offering bomb-shelter information that in fact delivered spyware — a novel fusion of digital and physical attack.

The single clearest example of a cyberattack designed purely for psychological effect is the BadeSaba prayer-app hijack: the widely used Iranian religious-calendar app, with more than five million downloads, was compromised at the very moment the 2026 strikes began to push defection messages to military personnel. CSIS reads this as Israel's integration of cyber and influence operations to inflame anti-regime sentiment, timed to sow confusion at the outset of the air campaign. The choice of a prayer app is the giveaway, since it reaches precisely the religious, pro-regime demographic one would want to demoralise. In parallel, Iran's IRNA news agency and government websites were hijacked to display anti-regime messages.

The most active Iranian persona, Handala — now formally attributed by the US Justice Department to Iran's Ministry of Intelligence and Security — oper-

ated by compromising soft targets and timing the publication of stolen data for maximum psychological impact, dumping the personal details of Israeli military and government personnel, leaking millions of voter records, publishing power-grid maps, and issuing death threats.

Taken together, the Iran wars validate the central theme: on both sides, cyber is used far more as an instrument to shape minds and morale — defection messaging and anti-regime injection from the Israeli side, fear and perception-hacking from the Iranian side — than as a war-winning physical weapon. Interestingly, this aligns well with the Iranian view of cyber-psychologic warfare as "soft war" (jang-e narm). It is defined as psychologic influencing and propaganda, which is used to destabilise the target country without the use of armed force.

Iran has prepared for cognitive warfare exceptionally well. Iran's National Information Network (NIN) is a prime example of this. It can be used as a replacement for the internet during crises by cutting connection to outside the country while still allowing domestic services to function. This way, the government can control the entire digital information space. It can be seen as a direct counter to foreign cyber-psychological operations.

An open analytical question is whether the psychological value of cyber is concentrated at the start of a campaign, as a shaping tool, or whether it can sustain pressure across a long war. The 2026 case suggests the influence-and-pressure use of cyber did sustain over months, but as event-driven pulses rather than a steady stream: tracking by SOCRadar found that daily attack claims peaked shortly after major kinetic strikes, and although many claims were exaggerated or duplicated, their sustained volume created psychological pressure and media amplification.

The best current read, triangulating across the Iranian and Israeli publics, is that a rally-and-resilience dynamic dominated on each side, so that the psychological cyber operations largely failed to shift mass sentiment in the intended direction even as they produced real local effects — fear spikes, some successful recruitment, and, in Iran, a manufactured appearance of unity. This is, notably, the same conclusion Ukraine points to: measurable psychological distress, but resilience absorbing most of the strategic blow.

»

Conclusion

Across all of these conflicts a single conclusion recurs. The psychological dimension of cyberattacks is not an incidental by-product of operations aimed at other ends; increasingly it is their primary purpose, with the human mind as the intended target. Cyber-psychological operations reliably produce the effects their designers seek at the individual level — fear, distress, a sense of violation, and eroded trust — and they can be tightly integrated with conventional military action. Yet at the societal level they have repeatedly fallen short of their strategic goal, because national resilience has tended to absorb the blow, and because rally effects often push public sentiment in the opposite direction. Compounding this, the specific contribution of any single cyber operation is extremely hard to isolate from everything else happening in a live war. The mind may be the

payload, but it has so far proved a remarkably resilient target. When it comes to individuals and organisations, however, anticipating significant psychological effects from cyberattacks should become the norm. They usually lack the level of resilience societies have, and the psychological repercussions can therefore be much more severe. In the middle of a crisis caused by a cyberattack, organisations should pay more attention to their employees’ psychological wellbeing. The situation might be dire, and extra effort is often required from everyone to mitigate the damage, but pushing too hard can end up damaging the employees instead. Mental resilience has been nominated as one of the vital pillars of the Security Strategy of Finland. In the future, its importance will be emphasised even further, and more attention must be paid to cyber-psychologic influencing.



SOURCES :

<https://databreachclassaction.io/blog/the-psychological-impact-of-data-breaches-on-victims>
<https://journals.sagepub.com/doi/10.1177/13691481231210383>
<https://www.tandfonline.com/doi/full/10.1080/19331681.2024.2420669#abstract>
<https://academic.oup.com/jogss/article/8/1/ogac042/6988925?login=false>
<https://www.bleepingcomputer.com/news/security/from-cipher-to-fear-the-psychology-behind-modern-ransomware-extortion/>
<https://puolustusvoimat.fi/documents/1951253/2815786/2025-3%20Psychological%20effects%20of%20cyberattacks.pdf/9d278114-e577-7359-2c9b-40750b6976be?t=1741783617259>
<https://www.techradar.com/pro/the-aftermath-of-the-kyivstar-cyber-attack-is-a-warning-for-us-all>
<https://besacenter.org/the-cyber-domain-in-the-russo-ukrainian-war/>
<https://besacenter.org/the-cyber-domain-in-the-russo-ukrainian-war/>
<https://www.esecurityplanet.com/threats/the-shadow-war-predatory-sparrow-vs-irans-infrastructure/>
<https://www.usnews.com/news/politics/articles/2026-03-29/hacked-hospitals-hidden-spyware-iran-conflict-shows-how-digital-fight-is-ingrained-in-warfare>
<https://www.csis.org/analysis/how-will-cyber-warfare-shape-us-israel-conflict-iran>
<https://zendata.security/2026/03/02/cyber-warfare-in-the-us-israel-vs-iran-conflict-roaring-lion-epic-fury/>
<https://www.rusi.org/explore-our-research/publications/commentary/fog-proxies-and-uncertainty-cyber-us-israeli-operations-iran>
<https://raaznet.com/en/reports/inside-irans-national-information-network>
<https://www.chathamhouse.org/2026/01/irans-internet-shutdown-signals-new-stage-digital-isolation>
<https://bit.sbu.ac.ir/Lab/ByFaculty>
https://ds.sndu.ac.ir/article_562.html
<https://civilica.com/doc/633994>
<https://civilica.com/doc/539792>
https://ds.sndu.ac.ir/article_562.html
<https://yle.fi/a/3-12152682>



Services

Cyberwatch Finland is a reliable and competent partner and service provider in cyber management and strategic cybersecurity.

Cybersecurity Capacity Building

Cyberwatch Finland is a strategic cybersecurity consultancy house that serves companies and other organisations by developing their ability to anticipate and prevent cyberattacks. The company was founded in February 2017. Cyberwatch Finland became a part of Netum Group Plc 21st of April 2026. We help companies and organisations with flexible solutions, quality services and with wide knowledge base.

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.

Our Services



- Web Analysis - darkSOC® and Attack surface analysis
- Operational Environment Analysis (Weekly and Monthly Reviews)
- Thematic and Special Reports (on request)
- Training and competence development: Cyberwatch training modules and lectures, Cyber situational awareness for the personnel, tailored training package (tailored by organisation or role-based)
- Management advisory services and Cyber Due Diligence (e.g. different scenario or crisis management work shops)
- AI-assisted Cyber risk management model
- NIS2 Consulting Service

We create added value for you:

- 1 With our dark and deep web services we are cutting edge in building prevention capabilities for organisation
- 2 We produce organisation-tailored up-to-date situational awareness and threat intelligence information
- 3 We build smart cybersecurity services, and our main focus is on agile and effective cyber risk management processes

Cyberwatch Finland's Cybersecurity Services

- For all stages of a company's life cycle



1. STARTING POINT

- Cyber maturity checking by making Cyber Maturity Analysis
- Web analysis (darkSOC®), Attack surface analysis & Operational environment analysis

2. ESTABLISHING OPERATIONS AND TRAINING

- Training
- Cybersecurity Regulations & Guidelines
- NIS2 Business Consultation
- Cybersecurity Development Plan

3. MAINTAINING A SITUATIONAL AWARENESS

- For management and personnel
- Operational environment analysis: weekly and monthly review

4. DEVELOPMENT AND MAINTENANCE OF CYBER RISK MANAGEMENT & CYBER SITUATION MONITORING

- Cyber risk management plan
- Maintaining situational awareness (e.g. continuous monitoring of Web analysis)
- Providing additional training

5. SUPPORTING DEVELOPMENT

- Supply Chain Auditing
- Background Investigations
- Cyber Due Diligence
- Cyber risk-based decision-making (scenario exercises)

6. CONTINUITY MANAGEMENT

- Management Consulting Services
- Monitoring and developing cyber risk management measures
- Scenario Based Cyber Crisis Management Exercise

Organizational challenges

- ! Rapidly Evolving Cyber Threats
- ! Limited Visibility Into Risks
- ! Increasing Regulatory Requirements (NIS2)
- ! Cyber Risks of Supply Chains

Our Solutions

- ✓ Cyber Threat Situational Awareness Service
- ✓ Strategic Analysis and Cyber Threat Intelligence
- ✓ Easy-to-Use Cyber Risk Management Model
- ✓ Dark and Deep Web Analysis (darkSOC)

Cybersecurity is often relegated to the IT level, even though it should be a part of strategic risk management.



Resilient business & crisis preparedness
Cybersecurity, defence & the European security landscape
Trusted digital society & democratic security

CYBER SECURITY NORDIC

28–29 Oct 2026

Helsinki Expo and Convention Centre

/MESSUKESKUS



Ron Deibert

Founder and Director,
Citizen Lab,
University of Toronto



Susann Lüdtkke

CEO & Founder,
L.I.A. – Lüdtkke Intelligence
& Analytics



Paolo Palumbo

VP, Strategic Threat
Intelligence & Research,
WithSecure™



Holger Haljand

CEO,
Telia Finland Oyj



Leading nordic meeting place for cybersecurity leaders, experts and decision-makers. And this is only the beginning. More than 80 leading cybersecurity and information security experts on stage. Explore the full event at cybersecuritynordic.com