



Cyberwatch Finland

MAGAZINE 1/2025



Cybersecurity is Built by Small Actions and Management of Large Concepts



A Passion for a Safe Cyber World



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, PhotoShopAI
PRINT Scanseri Oy, Helsinki

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

CONTENT

4



Editorial

 **AAPO CEDERBERG**

6



The Operating Environment of the
Cybersecurity Industry in 2025

 **RISTO RAJALA & PETER SUND**

11




National cyberspace
and cyber operations

 **MARTTI LEHTO**

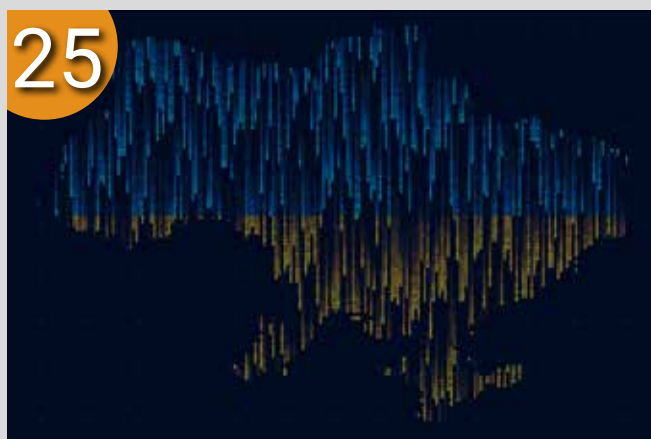
19



Legislation as an instrument
of cognitive warfare

 **PETER B.M.J. PIJPERS**

25



Weekly review 9/2025

 **War in Ukraine special**

35



Monthly review
March/2025

48





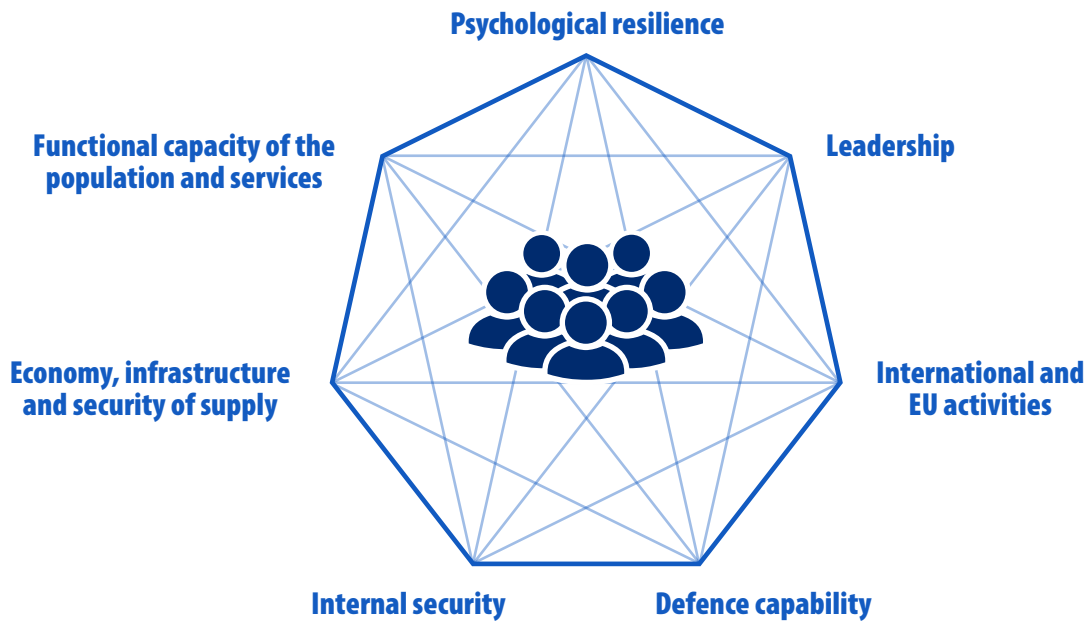
War accelerates development – can we keep up?

History has shown that technology develops much faster in war and crisis situations than in normal societal conditions. The war in Ukraine is not an exception. The impact can be seen in both military technology and dual-use products. The mass use of drones for both intelligence and influencing operations has also changed the planning of operations and combat tactics. Critical infrastructure has been the target of continuous kinetic influencing and cyber operations. Nevertheless, many experts are of the opinion that mobile phone networks are currently working better in Ukraine than before the war.

The image and methods of war have also changed. At the same time there is a traditional war of destruction as well as information, cyber, energy, economic and hybrid warfare. All critical sectors of society can be seen as the scene of war. Modern social structures contain goals and weaknesses that can be attacked to achieve the desired political, economic, military and cognitive effects. The question arises whether these different forms of warfare can be used to win a war, or in general, can victory or win be defined. Traditionally, the winners of the war have gained control over the conquered territories and the right to control and dictate the political decisions of the defeated party. Even today, this seems to be the goal of Russia's war

of aggression. It seems that the war can only be won by kinetic operations. The question arises: what is the significance of these other forms of warfare?

Some experts in the art of war argued that future wars can be won through cyber warfare, or operations in space. In the light of the experiences gained from the war in Ukraine, it seems that this is not the case, but that these various forms of warfare mainly play a supporting role in winning a traditional war. Another perspective is how to wage a war without declaring a war while at the same time staying below the threshold of traditional war, i.e. when kinetic force is only used or is wanted to be used in e.g. various sabotage operations. The



Picture:
p. 16 "PUBLICATIONS
OF THE FINNISH
GOVERNMENT 2025: 3
Figure 2. The vital functions
of society."

concept of hybrid warfare has been developed for this very purpose, it wants to achieve the goals of the war without the use of military force, i.e. to win the war without firing a single shot.

European countries, Finland included, are the target of information and cyber operations every day. Russia and other actors that cause instability want to influence our political decision-making, the functioning of the welfare state and the opinions of citizens by causing fear and uncertainty to citizens' everyday services and quality of life. Every serious cyberattack has information effects in both the short and long term. A good concrete example of this, is the attacks on banks and their online services, which make us to doubt losing our money and wealth.

In January, Finland published an updated security strategy for society. It is already the fifth update of the comprehensive security model for society. The concept and key principles have remained largely unchanged and form the basis to society's preparedness and resilience to crises. Perhaps the most significant change in strategy is putting people at the center of the strategy diamond and moving mental crisis resilience to the

top corner of the diamond. This is certainly justified when viewed from the perspective of warfare and modern forms of influencing. The war will be won if the soldiers' will to fight remains high and civil society is able to secure its' vital functions in all circumstances.

More than 80 percent of successful cyberattacks are caused by human activity in one way or another. We make mistakes either by accident or through our incompetence. In other words, training is still the most powerful tool in cybersecurity. The leap in technological development also requires a leap in the development of people's skills. A war cannot be won with technology alone, there is always a need for top experts and competent users of technology. The importance of mental crisis resilience cannot be overemphasized, and even that can be improved by good competence. Hopefully, now and in the future, different elements in addition to war will also accelerate and motivate us humans to adopt new skills and work together more effectively.

This publication has been produced in cooperation with The European Centre of Excellence for Countering Hybrid Threats. I would like to thank them for a wonderful

and fruitful cooperation and for the excellent articles published in this journal. Special thanks goes to Dr. Josef Schröfl, with whom we have had excellent cooperation for seven years now. These articles are based on the 6th Cyber Power in Hybrid Warfare Symposium held in the spring of 2024 under the leadership of Josef Schröfl.



The Operating Environment of the Cybersecurity Industry in 2025



RISTO RAJALA &
PETER SUND



The Finnish cybersecurity industry entered the year 2025 in an ever-changing operating environment. The new national cybersecurity strategy and its forthcoming implementation plan, as well as decisions regarding the use of public funds, will shape the domestic environment. However, the most significant impact comes from the new EU regulations that have reached the implementation phase, forcing more companies and organizations to invest in managing their digital risks, offering new business opportunities for companies providing cybersecurity products, services, and solutions.

National Cybersecurity Strategy in Place

The goal of the cybersecurity strategy, issued as a government resolution in October 2024, was to update the strategy to reflect the changed operating environment and the government program's entries, as well as to meet the requirements of the NIS2 directive. Finland's cybersecurity strategy is an important document, not only from the perspective of EU law requirements but also because it can guide policy actions, the development of cooperation between administration and various actors, and the careful and effective use of public funds. The commitment of public administration to the development of cybersecurity is naturally essential for promoting the digital security of our society. The most important thing would be to choose measures based on the impact of cybersecurity risk management. Unfortunately, the strategy partly gives the impression that the purpose was rather to list what the authorities themselves would like to do and what resources they would want for themselves. It is widely known and indisputable that Finland's economy, both private and public, is in significant difficulties, and no improvement is expected in the short term. Necessary adjustments to public finances are likely to continue throughout this decade. This fact has not sufficiently influenced the thinking of the civil service, even though the need is compelling and political guidance exists.

The resourcing, implementation, and monitoring of the strategy are crucial for success, which directs attention to the implementation plan of the national cybersecurity strategy. The resources linked to the implementation of the strategy determine how the goals presented in the strategy are achieved. It would be justified to have the targeted actions prioritized and resources allocated in the implementation plan. This has been attempted, but the planning does not seem to have reached

the budget items in all respects. As the changed security situation in Europe will likely still require investments in armed defense capability and increasing debt, it is important for the comprehensive development of society's cyber resilience that the defense administration's actions included in the cybersecurity strategy are carried out with the administration's own funding, and that it is ensured that other sectors subject to savings, particularly the Ministry of Transport and Communications and the Ministry of Finance, due to their broadest impacts, can carry out their own actions.

More broadly, when examining the use of public funds, the budget cuts made in the Ministry of Transport and Communications' sector particularly stand out, negatively affecting the overall security of society when appropriate measures to improve the cyber resilience of the business sector and other (civil) society cannot be implemented. It is therefore important that military cyber defense actions do not take resources away from measures aimed at protecting the rest of society. A more balanced result would be achieved by more effectively utilizing the joint development budget for digitalization written in the government program and Finland's digital compass also for improving cybersecurity. The joint development budget can be used to concentrate resources and ensure that projects are in line with the priorities of the government program and interoperable with the entire state administration's digital infrastructure and digitalization development. The joint development budget was intended to be introduced this year according to the government program, but no confirmed decision has been made.

In connection with the project coordinated by the Ministry of Finance to assess the current state of compliance of information systems, the Defense Forces have expressed the need to develop an independent authority for the assessment and approval of information systems and

encryption products operating in connection with them. If the defense administration has extra resources for security assessment and approval activities, they could be used to support Traficom's resources within the core functions of the defense administration. From the perspective of the cybersecurity industry and the broader business sector, it is essential that new resources allocated to approval and assessment activities are primarily directed to the Cybersecurity Center of the Finnish Transport and Communications Agency Traficom, so that the benefits of the activities can be realized for the entire society. The assessment and approval activities planned to be considered in connection with the Defense Forces should primarily focus on assessing security obligations originating from NATO.

Key legislative and policy projects affecting the domestic operating environment of the cybersecurity industry this year will also include the goal decision on security of supply, the comprehensive reform of the Emergency Powers Act, and the overall review of regulation on disruptions and crisis situations in all administrative sectors, the assessment and development of police criminal intelligence legislation, the internal security report, and the defense report.

EU Direction Taking Shape

The steps of the European Union's new term are beginning to take shape. In the summer of 2024, the political guidelines for 2024-2025 of the European Commission President Ursula von der Leyen, who received an extension, were published, which can be seen as a kind of EU government program. The rest of the commission's composition was confirmed in November 2024, when Henna Virkkunen's appointment as the executive vice-president responsible for technological sovereignty, security, and democracy was con-

firmed. This is the most significant international position granted to a Finn in the history of our country and is particularly timely with the digitalization of societies, the development of disruptive technologies, and the unstable security environment. The position also includes cybersecurity matters, for which Virkkunen has a comprehensive approach to strengthening society's cyber resilience, the security-by-design operating model, the importance of the cybersecurity industry as a guarantor of the security of digital infrastructure, and the importance of small and medium-sized enterprises as developers of new innovations.

Commission President von der Leyen asked "three wise men" to prepare reports to support the commission's work and shape the agenda. The tasks were assigned to three former European heads of state: the report by former Italian Prime Minister Enrico Letta focused on the current state and development of the EU internal market, the report by former Italian Prime Minister and European Central Bank President Mario Draghi addressed strengthening EU competitiveness, and the report by former Finnish President Sauli Niinistö concerned EU military and civilian readiness. It is expected that the commission's future annual work programs will be defined according to the guidelines set by Letta, Draghi, and Niinistö's reports.

Draghi, Letta, and Niinistö all highlighted in their reports the simplification and harmonization of legislation on law enforcement actions by digital communication and telecommunications security authorities within the EU area. Harmonizing law enforcement legislation would benefit companies, but it is questionable how this could be practically implemented. Strong encryption requires that only the parties to the communication have access to the content of the communication. When discussing aspirations and development ideas,

it is essential to rely on technological realities. It is not possible to break strong end-to-end encryption (E2EE) that ensures the confidentiality of digital communication with the cooperation of communication service providers without seriously compromising cybersecurity. This theme is also strongly related to the technically unfeasible commission proposal for rules to combat online child sexual abuse, which FISC has actively influenced.

Against this background, for example, the Finnish Parliament has established Finland's position on the EU legislative proposal concerning online child sexual abuse:

"...the proposed model would actually lead to mass surveillance of communication and would mean a weakening of the regulation on the protection of the confidentiality of communication at the EU level. The Grand Committee considers that the proposed model would actually circumvent the purpose of using end-to-end encryption in communication, as the monitoring of CSA material would be technically carried out by requiring communication services using end-to-end encryption to enable the technical identification of transmitted messages already on the communicator's terminal device before the content of the message is encrypted...that Finland should not accept the compromise proposal of the presidency [Hungary] regarding the identification order...The Grand Committee requires that the government takes the above into account and that the government does not accept the proposed identification order."



In practice, the Finnish legislator understands well the values and technological risks associated with electronic communication. From the perspective of protecting children, opposing the legislative proposal does not mean supporting child sexual abuse or downplaying the problem. The choice is not between supporters and opponents of child sexual abuse, but rather whether to support the fight against child abuse with effective or ineffective means.

Economic security was strongly highlighted in all three reports. Solutions included reducing economic dependencies, securing supply and production chains, ensuring the availability of raw materials, and establishing closer trade relations with like-minded countries. Niinistö proposed a clear increase in public-private sector cooperation to reduce dependencies and economic pressure in foreign direct investments and outward investments. According to Niinistö, the EU must also maintain its ability to sustain critical infrastructure and ensure economic and cybersecurity, promoting innovation and technological leadership. Supporting companies in improving their cyber resilience was highlighted in Niinistö's report as part of strengthening public-private sector cooperation, but the proposed means focused solely on raising awareness, exercises, and training.

Strengthening the European defense industry was highlighted in all three reports: Through the promotion of defense internal markets

and European joint procurements, as well as the development of common capabilities (including cyber, space, air defense). Niinistö called for the establishment of an investment guarantee system that would encourage investments in Europe's defense technological industrial base. In March, the European Commission published the White paper on the Future of European Defense, intended to serve as a plan for re-arming Europe by 2030. The White Paper and the ReArm Europe plan represent a step forward in the development of European defense and security. They recognize the critical role of technologies such as artificial intelligence, cybersecurity, secure communication, and electronic warfare for Europe's security and resilience, along with joint procurements. This is in line with accelerating Europe's technological edge in military defense. The core idea of the White Paper is that the EU will become a credible, independent actor in defense by 2030.

The need for large projects of common European interest was emphasized in all three reports: Draghi called for the simplification of funding programs, the increase in the size of projects, and the reform and expansion of the European Innovation Council (EIC) to match the US Department of Defense's Advanced Research Projects Agency (DARPA), which utilizes public procurement in financing significant disruptive technologies. Letta mentioned strengthening European encryption solutions as one possible project.

The shortage of skilled labor was highlighted by Draghi and Niinistö as a critical issue – both from an economic and preparedness perspective: Draghi called for a focus on adult education and strengthening sufficient funding for member states and private organizations (including encouraging companies to allocate more resources to training, for example by offering tax incentives). Niinistö stated that the shortage of skilled workers in criti-

cal areas, particularly in the cybersecurity sector, threatens the EU's crisis resilience and requires measures. These include, according to him, mapping labor needs, training new employee segments, facilitating labor immigration, and developing mechanisms for labor mobility in crisis situations.

There has been much talk about the new EU regulations, and for good reason: they represent one of the most significant developments shaping the operating environment in the history of the cybersecurity industry. The Cyber Resilience Act, which sets minimum security requirements for devices and software connected to the network, and the NIS2 directive, which imposes obligations on critical companies and organizations to manage digital risks and report security breaches, are the most important new regulations for cybersecurity. However, the EU Cyber Solidarity Regulation will also impact the business of many cybersecurity companies, as the funding it provides allows critical entities in member states to improve their cybersecurity by utilizing the products, services, and solutions of trusted companies included in the "cybersecurity reserve."

Successful and consistent implementation of the new EU legislation is a crucial step towards a genuine and comprehensive culture of public-private sector cooperation to ensure readiness and crisis resilience – while remembering the limitations on the transfer of public power. The new commission must significantly invest in supporting and accelerating standardization, increasing awareness and cooperation between member states, and providing financial support from EU funding programs. The most important and primary practical measure would be to increase and channel EU grant funding to member states for the adoption of modern security solutions in companies, especially for the implementation of risk management measures under the NIS2 and CER directives.



Internationalization in an Unpredictable World

The international operating environment is becoming increasingly challenging and difficult to predict. The actions of authoritarian states, particularly China and Russia, challenge the Western world and the rules-based international order, and observing the actions of the new US administration leaves it unclear what role the US will pursue globally in the future, and above all, by what means. It is also open who will benefit and who will suffer – including the US itself. International trade and security policy issues are extremely significant for domestic cybersecurity industry companies. Internationalization aimed at exports is a prerequisite for the profitability of cybersecurity industry companies and the ability to invest in research, development, and innovation. The international market for cybersecurity industry products and services is growing by an estimated 15-20 percent annually, according to the European Commission. Finland has internationally recognized, even unique expertise in several areas of the cybersecurity industry, which has significant export potential.

The government is preparing a reform of the Team Finland business services' foreign network, where Business Finland's foreign operations will be integrated into the foreign affairs administration. FISC supports the reform, and the goal set by the Minister for Foreign Trade and Development Ville Tavio to "provide companies with even better export promotion services, created in cooperation with the business sector and staff." Considering the needs of the business sector, especially growing industries with significant export potential, in the reform of export promotion services is particularly important. Services are most beneficial when tailored and optimally targeted to the needs of export companies. Our goal is that when reforming serv-

es, a model is created where FISC and other industry organizations of growing industrial sectors are systematically consulted to support the definition of operational priorities, for example, identifying the most potential target markets, current themes of the industry, and factors hindering market access.

The task of FISC's advocacy is to bring the needs of the cybersecurity industry operating in Finland to the attention of political decision-makers and civil servants, as well as to broader awareness. In discussions and development projects concerning the strengthening of society's overall security, we emphasize the critical importance of a strong economic and industrial base, healthy competition, international competitiveness, and favorable investment conditions for our country's security and supply security. At the same time, we strive to ensure that harmful actions to these pillars of supply security and national security are avoided. To quote NATO's highest military leader, Admiral Rob Bauer: "Armies win battles, but the economy wins wars." In other words, a patriotic act is to conduct successful business.

FISC provides information to its members about the ever-changing operating environment broadly through member bulletins, and we also organize events on various current topics ourselves and together with our partners, not forgetting the participation opportunities we offer, for example, in certain state administration and European cooperation organizations' events. In 2024, we started the joint "Cyber Industry in Transition" concept together with Traficom's Cybersecurity Center and the National Emergency Supply Agency, within which we have organized informational webinars on current cybersecurity topics, such as the EU Cyber Resilience Act, AI security perspectives, and quantum-safe encryption. The webinar series has been very popular and has attracted thousands of viewers over the past year. Cyber Industry in Transition and other activities of our association continue, and we gladly welcome suggestions from our members for their and other advocacy development. Our association is open to companies and organizations operating in the field of cybersecurity.



PETER SUND

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



RISTO RAJALA

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

Jukka Rapo



MARTTI LEHTO

National cyberspace and cyber operations

Abstract:

Historically, warfare has occurred in various operating environments, traditionally referred to as domains: land; sea; air; and outer space. In recent times information and cyberspace have emerged as additional domains. National cyberspace can be categorized in six dimensions: military; political; economic; societal; technological; and citizen. Offensive cyber operations are increasing in diversity, sophistication and frequency. The availability of disruptive technologies to both attackers and defenders has heightened the complexity of these attacks and made attribution more challenging. This is particularly evident in Russia's cyber operations in Ukraine.

Problem statement:

How can Russian cyber operations be understood as part of hybrid operations?

Bottom line upfront:

States should ensure that activities in cyberspace improve cybersecurity dialogue, involve all relevant civil society organizations in building cybersecurity, and increase research, education and training in the field.



So what?

Extensive international cooperation is needed to build national cyber resilience. Key organizations involved in this cooperation include NATO and the EU. For example, the EU Cyber Solidarity Act will enhance preparedness, detection and response to cybersecurity incidents across the EU. Cybersecurity should be viewed broadly as a theme that cuts across digital society, necessitating the integration of cybersecurity and cyber defence into a comprehensive security framework.



THE PARADIGM HAS CHANGED, AND THE CHANGE CONTINUES

In the traditional warfare model nation states engage in conflict for various reasons tied to their national interests. Warfare is understood as occurring in the diverse domains or operational environments where military operations take place. These activities can be divided into kinetic actions with physical effects and non-kinetic actions.

The non-kinetic environment has evolved over the last 100 years, transitioning from radio to computer technology and Artificial Intelligence (AI). It comprises largely undetectable silent technologies capable of inflicting damaging, debilitating and degrading physical and neural effects on unwitting targets.[1]

Cognitive warfare involves understanding and influencing human perception, cognition and behaviour to achieve strategic objectives. Emerging technologies such as AI, especially generative AI, and neuro-technologies enable highly accessible and efficient subversion within the cognitive domain of warfare. The mass production of data and automated content creation have led to an abundance of publicly available data that can be used for cognitive manipulation. Consequently, data and AI algorithms have become weapons of cognitive warfare.[2]

UNDERSTANDING NATIONAL CYBERSPACE

Cyber threats are complex and asymmetrical because digital cyberspace is borderless and multidimensional. The national cyber environment consists of various actors and functional entities. The cyber environment differs from the traditional national operating environment, where an independent state has clearly defined geographical boundaries – land, sea and airspace – that determine its jurisdiction.

Political dimension

The political dimension of national cyberspace represents the policy processes, legislative frameworks and regulations designed to promote, direct and control cybersecurity. The political nature of cyber issues is increasingly emphasized in both national and international politics. Cybersecurity issues are being presented more broadly and with greater significance in international fora and organizations such as the EU, NATO and the OSCE.

Like other diplomatic efforts, cyber diplomacy involves building strategic partnerships with countries globally to enhance collective action and cooperation against shared threats. This includes assembling coalitions of like-minded nations on vital policy issues, sharing information and national initiatives, and confronting bad actors. Cyber diplomacy employs diplomatic tools and initiatives to achieve objectives in cyberspace. Its goals include minimizing the consequences of cyber aggression such as cyber espionage and offensive cyber operations carried out by state or non-state actors. Additionally, it aims to address international law and norms in the field of cybersecurity and undertake actions that build trust. Mutual understanding and common

rules can reduce the threat of various conflicts.[3]

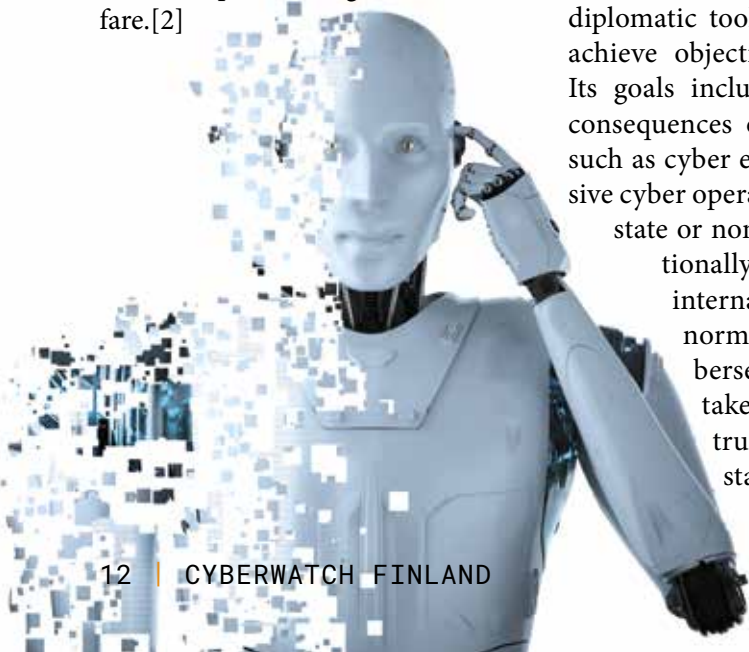
The EU has produced several key frameworks and policies, including the Diplomatic Response Framework (Cyber Diplomacy Toolbox, 2017), the Cyber Defence Policy Framework (2018), the EU Cybersecurity Act (2019) and the Council Decision (2019) concerning restrictive measures against cyberattacks threatening the Union or its member states. Furthermore, following the EU's Cybersecurity Strategy for the Digital Decade, the bloc has introduced several acts and policy papers such as the NIS 2 Directive, the European Cyber Resilience Act, the Digital Operational Resilience Act, the European Cyber Defence Policy, the Strategic Compass of the European Union and the European Chips Act.[4]

Similarly, the EU Cyber Diplomacy Toolbox is a collective diplomatic response to malicious cyber activities. It is part of the EU's approach to cyber diplomacy within the Common Foreign and Security Policy. Its goal is to contribute to conflict prevention, mitigate cybersecurity threats and promote stability in international relations.[5]

Military dimension

As part of their military strategy, several nations are developing their capability of conducting operations in cyberspace, alongside land, sea, air and outer space. At the strategic level of cyberwarfare one state aims to influence the vital functions of another. Cyber operations are integrated with other military forces at the operational and tactical levels.

NATO has long considered cyber defence a key component of its overall defence strategy. NATO's strong focus on cyber defence began at the 2002 NATO Summit in Prague. NATO and its allies are responding to cyber threats by enhancing their



ability to detect, prevent and respond to malicious cyber activities. Strong and resilient cyber defences are crucial for NATO and its allies to fulfil the Alliance's three core tasks: deterrence and defence; crisis prevention and management; and co-operative security.[6]

At the 2023 NATO Summit in Vilnius member nations endorsed a new concept to enhance the contribution of cyber defence to NATO's overall deterrence and defence posture. They also launched NATO's Virtual Cyber Incident Support Capability (VCISC) to support national mitigation efforts in response to significant malicious cyber activities.[7]

Defence forces need efficient cyber resilience, non-kinetic power convergence, and the capability of operating in and through contested and congested cyberspace. Two factors, cyber power and cyber deterrence, unite the military and political dimensions of cyberspace. The National Cyber Power Index describes a nation's ability to operate in a global cyber environment. [8] Cyberspace deterrence aims to influence an adversary's behaviour, discouraging them from engaging in unwanted activities.[9]

Societal dimension

The current decade of digitalization and data economy transformation is changing the world. This change affects us all, as digitalization and data are part of everyday life in every sector of society. This is reflected in new types of services, operating models, technologies and skill requirements. Digitalization covers virtually every area of welfare, including social services, the education sector and healthcare services.

The asymmetrical threat posed by cyberattacks and the inherent vulnerabilities of cyberspace constitute a serious security risk. In the cyber world one of the most important threats focuses on critical

infrastructure (CI). CI includes the structures and functions vital to society's uninterrupted functioning, comprising both physical facilities and electronic functions and services such as political decision making, internal and external security, logistics, the economy, energy, telecommunications, and food production. In recent years, attacks against CI, critical information infrastructures and the internet have become increasingly frequent and complex as perpetrators have become more professional. Attackers can inflict damage on physical infrastructure by infiltrating the digital systems that control physical processes, damaging specialized equipment and disrupting vital services without a physical attack.[10]

A focus in the social dimension is Critical Infrastructure Protection (CIP), which involves actions taken to prevent and mitigate the risks resulting from the vulnerabilities of critical infrastructure assets and to facilitate recovery in the event of an attack.

Citizen dimension

Digital technologies have become deeply integrated into human life. The operational reliability of information and communications technology is essential for the smooth functioning of modern society, the security of its infrastructure and the wellbeing of its citizens. It is also crucial for maintaining public trust in societal operations. In a digital society citizens need to act safely and responsibly in the face of digital threats. Digitalization offers significant benefits, making life more efficient and enabling global communication. However, it also has impacts on citizens' private, social and public lives, influencing their privacy, autonomy and security.[11]

According to the EU Digital Compass, "Digital technologies should protect people's rights, support democracy, and ensure that all

digital players act responsibly and safely. People should benefit from a fair online environment, be safeguarded against illegal and harmful content, and be empowered when interacting with new and evolving technologies like artificial intelligence. The digital environment should be safe and secure for all users, from childhood to old age, ensuring empowerment and protection."[12]

The digital skills targets set by the Digital Decade are still far from being achieved, with only 55.6 per cent of the EU population having at least basic digital skills. Member states are progressing towards the target of making all key public services and electronic health records accessible to citizens and businesses online, as well as providing them with secure electronic identification (eID). However, achieving 100 per cent coverage of digital public services for citizens and businesses by 2030 remains challenging.[13]

Economic dimension

Cybersecurity Ventures is a prominent industry research and media organization recognized for its authoritative insights and contributions to cybersecurity. Based on its report, global cybercrime costs will increase by 15 per cent annually over the next five years, reaching USD 10.5 trillion per year by 2025. This would represent the largest transfer of economic wealth in history. Cybercrime costs encompass a range of issues, including damage to and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, disruption to normal business operations following an attack, forensic investigation, data and system restoration and deletion, and reputational damage.[14]

The global financial system depends increasingly on digital infrastructure. The economic impact of

cyberattacks includes not only the direct costs to organizations but the long-term effects on national economies and the expenses related to enhancing cybersecurity at various levels. Preparing for cyberattacks can also influence taxation and public expenditure if additional resources are needed for cybersecurity in the public sector. Developing cybersecurity thus requires careful consideration from both economic and societal perspectives.[15]

Regulatory mechanisms can improve cybersecurity but also come with their own set of challenges. For example, preventive regulations, post-incident obligations and information access requirements provide various benefits and costs. The NIS 2 Directive is an example of such a regulatory approach because it provides legal measures to

boost the overall level of cybersecurity in the EU. Political, societal and economic dimensions all play a role in achieving economic and financial stability. Effective public administration is crucial for maintaining democracy and ensuring societal welfare.

Technological dimension

Information and communications technology (ICT) encompasses a range of fields related to computer systems, software, hardware, and data processing and storage. One of the primary goals of ICT tools and systems is to enhance how individuals and organizations create, process and share data and information. ICT plays a crucial role in various areas, including business, education,

healthcare, defence and leisure activities.[16]

Digital tools and software streamlining processes in business reduce manual operations and enhance online customer service. They enable businesses to automate tasks, improve efficiency and productivity, protect customer information, and build an information ecosystem. Digitalization also brings new threats, however. The cyber world attracts criminals seeking opportunities to steal, exploit and sell information. Cybersecurity solutions must be smart and effective to protect both citizens and organizations from these emerging threats.

Trust is a fundamental aspect of a digital society. Trust must be established and upheld for a digital society to fulfil its purpose and maintain social stability.



CYBER OPERATIONS AS PART OF HYBRID OPERATIONS

Hybrid operations incorporate several elements of cyber operations, aiming to remain below the threshold of armed conflict. Intentional instability can be maintained through cyber operations in both peacetime and wartime. Russia's hybrid warfare strategy can be described as a creative application of force that combines a broad spectrum of military and non-military tools and vectors of power across an extensive multi-domain battlespace.

According to the NATO Washington Summit Declaration (2024), "Russia's full-scale invasion of Ukraine has shattered peace and stability in the Euro-Atlantic area and gravely undermined global security. Russia remains the most significant and direct threat to Allies' security." [17]

Political dimension

Russia is employing hybrid measures to influence the politics and policies of countries in the West and beyond. This strategy represents a significant challenge for Western governments. Russia aims to ensure that political outcomes in targeted countries are aligned with its national interests. Countries with weak legal and anti-corruption frameworks, or where domestic groups share Russia's interests or worldview, like Moldova, are particularly vulnerable. The Kremlin is capable of influencing elections and other political outcomes beyond its borders. The Russian theory of strategic culture explores and explains Russian offensive cyber operations such as cyberattacks and cyber espionage. Elements of Russian strategic culture related to these operations include asymmetric means of warfare and the denial, deception and concept of tactical truth. Russia's ongoing aggression in Ukraine highlights its continued threat to the rules-based international order. It is assumed that Rus-

sian offensive cyber capabilities are now being developed to achieve the same performance in these Western tactics, techniques and procedures. [18] [19]

President Alexander Stubb of Finland has frequently addressed Russia's hybrid influence in his speeches, maintaining that Russia aims to destabilize societies through various forms of attack. He has also noted that modern conflicts often involve a mix of conventional and hybrid warfare and cyberwarfare, with hybrid attacks occurring frequently. In a speech at the Hertie School in Berlin on 8 May 2024, Stubb remarked, "Hybrid attacks are commonplace in peacetime, and they rarely come with a declaration of war. Traditional war is also complex and multifaceted. Conventional warfare still exists – as evidenced in both Europe and the Middle East – but the instruments and methods extend beyond mere shells and trenches." [20]

Military dimension

The use of cyber tools as a military strategy to target enemy forces and capabilities can be categorized similarly to other military operations. Cyber tools can be employed in conventional operations such as those observed in Ukraine or in more specialized operations like the Stuxnet attack against Iran. In these hybrid warfare operations methods are used to achieve specific objectives, often in a covert manner that, like special operations, falls below the threshold of traditional armed conflict. In war the objective of conflating kinetic tools and non-kinetic tactics is to optimally inflict paralysis and damage on an opponent's environment. [21]

Russia's invasion of Ukraine highlights the significant role cyber capabilities play in modern warfare, demonstrating how cyber tools can

complement conventional military strategies. The Russian approach includes notable operations that have affected targets beyond Ukraine, as well as various aspects of Ukrainian infrastructure, government and civilian networks. The CyberPeace Institute has recorded 2,258 cyberattacks and operations, 666 of which were targeted at Ukraine, and 2,258 at other countries. These cyber incidents targeted 23 different critical infrastructure sectors, affecting Ukraine and some 49 other countries. [22]

At an event in Canada in June 2024 NATO Secretary General Jens Stoltenberg remarked: "The challenge is that we are threatened by something which is not a full-fledged military attack, which are these cyber, hybrid is below Article Five, as is often referred to, threats, and that is everything from meddling in our political processes, undermine the trust in our political institutions, disinformation, cyber-attacks, we have seen across Europe and how many sabotage actions against critical infrastructure, and so on." [23]

Societal dimension

The development of cybersecurity requires a focused long-term effort. Risks can materialize rapidly, and the operating environment is constantly evolving. In recent years attacks on critical infrastructure, including information systems and the internet, have become more frequent, complex and targeted as attackers have grown more professional. They can inflict damage on or cause disruptions to physical infrastructure by infiltrating digital systems that control physical processes, damaging specialized equipment and disrupting vital services without a physical attack. These threats continue to evolve in their complexity and sophistication.

Russia may target cyberattacks against critical infrastructure to create uncertainty and mistrust among citizens and demonstrate its capability of paralysing essential societal functions. Even as Russia focuses on cyber operations related to the Ukrainian conflict, it remains a persistent global cyber threat. For example, goals have been the telecommunications sector (Triolan and Vinasterisk ISP, Ukrtelecom, Kyivstar), broadcasting companies, media, transport and logistics providers, data centres, the energy sector, and border protection.[24] [25] [26]

Moscow uses cyber disruptions as a foreign policy tool to influence other countries' decisions. It is continuously refining its espionage, influence and attack capabilities against various targets. Russia can target critical infrastructure, including underwater cables and industrial control systems, both in the United States and in allied and partner countries. During 2024 Russia's cyberattack targets have:[27]

- focused on German political parties and German military officials;
- launched an espionage campaign against the embassies of Georgia, Poland, Ukraine and Iran and a ransomware attack against Sweden's digital service provider for government services;
- hacked Microsoft corporate systems and 65 Australian government departments and agencies, stealing 2.5 million documents in Australia's largest government cyberattack; and
- hacked residential webcams in Kyiv to gather information about the city's air defence systems before launching a missile attack on Kyiv.

Citizen dimension

The citizen dimension emphasizes the impact of information. Attackers can systematically spread disinformation

through targeted social media campaigns to radicalize individuals, destabilize society and control the political narrative.

Russia's disinformation and propaganda ecosystem encompasses various official communication channels, social media, proxy sources and unattributed platforms used to create and amplify false narratives. This ecosystem consists of five main pillars: official government communications; state-funded global messaging; the cultivation of proxy sources; the weaponization of social media; and cyber-enabled disinformation. The Kremlin employs these tactics and platforms as part of its strategy of weaponizing information. Such disinformation and propaganda organizations include:[28] [29]

- The Strategic Culture Foundation, an online journal registered in Russia directed by Russia's Foreign Intelligence Service (SVR);
- Global Research, a Canadian website that is part of Russia's disinformation and propaganda ecosystem;
- New Eastern Outlook, a pseudo-academic publication of the Russian Academy of Science's Institute of Oriental Studies that promotes disinformation and propaganda focusing primarily on the Middle East, Asia and Africa;
- News Front, a Crimea-based disinformation and propaganda organization providing an "alternative source of information" for Western audiences;
- SouthFront, a multilingual online disinformation site registered in Russia that focuses on military and security issues;
- Katehon, a Moscow-based quasi think tank focusing on anti-Western disinformation and propaganda; and
- Geopolitica.ru, a platform for Russian ultranationalists that spreads disinformation and propaganda targeting Western audiences.

Economic dimension

Without dedicated action the global financial system will become increasingly vulnerable as innovations, competition and disruptive technologies continue to drive the digital revolution. While many threat actors are motivated by financial gain, a growing number of state-sponsored attackers are also launching disruptive and destructive attacks against financial systems.

Cybersecurity is crucial for maintaining economic and financial stability. For example, Russia seeks to influence European politics both directly and indirectly and has used energy as a tool of foreign policy. Cyber operations targeting critical infrastructure and economic systems can further destabilize economic and financial stability. As an MP, Rishi Sunak analysed possible Russian hybrid attacks in December 2017, saying, "Sabotage of undersea cable infrastructure is an existential threat to the UK. The result would be to damage commerce and disrupt government-to-government communications, potentially leading to economic turmoil and civil disorder." [30] [31]

The effective protection of the global financial system is primarily an organizational challenge. While efforts to strengthen defences and tighten regulations are important, they are insufficient to keep pace with the growing risks. Unlike many sectors, the financial services community generally has the necessary resources and technical capabilities. The key challenge is to coordinate cybersecurity protection across governments, the financial authorities and industry, as well as to leverage existing resources effectively and efficiently.[32]

Technological dimension

An attack vector is a path or means by which an attacker can gain unauthorized access to a computer,

network or IT/OT infrastructure to deliver a payload or malicious action. Attack vectors allow attackers to exploit system vulnerabilities.[33]

Between December 2021 and March 2022 US CYBERCOM's joint forces, in close cooperation with the government of Ukraine, conducted defensive cyber operations alongside Ukrainian Cyber Command personnel. This effort was part of a broader initiative to enhance cyber resilience in critical national networks. The teams implemented a threat-hunting operation in Ukraine, as well as remote analytic and advisory support, using inno-

vative techniques. They also conducted network defence activities aligned to critical networks. They identified 90 instances of malicious code the Russians had created to disrupt Ukrainian infrastructure. The teams also gained a valuable insight into adversaries' tactics, techniques, procedures, plans, capabilities and tools.[34]

Russian cyber threat activity against Ukraine has been carried out by various actors associated with the three main Russian security services: the Federal Security Service (FSB); the Foreign Intelligence Service (SVR); and the Main Intel-

ligence Directorate (GRU). These cyber actors have engaged in various threat activities against Ukraine, including disruptive and destructive cyber operations.

Prosecutors at the International Criminal Court (ICC) are investigating alleged Russian cyberattacks on Ukrainian civilian infrastructure as possible war crimes. ICC prosecutors are working with Ukrainian teams to investigate attacks that endangered lives by disrupting power and water supplies, cutting connections to emergency responders, or disabling mobile data services that transmit air raid warnings.[35]

TOWARDS COGNITIVE WARFARE

Hybrid threats aim to exploit a country's vulnerabilities and often seek to undermine fundamental democratic values and liberties. The digital cyber world can be divided into six interacting dimensions, with human beings at the core of each. In these dimensions people act as politicians, decision makers, operators, soldiers, developers, citizens and more. Cognitive superiority and cognitive warfare permeate all these dimensions, indicating a shift from purely kinetic approaches towards subversion.

The internet and social media are today among the most powerful

tools in cognitive warfare, targeting key figures, niche groups and the public. Social media platforms have become crucial battlegrounds, influencing and manipulating public perceptions, opinions and behaviours. Artificial intelligence has the potential to revolutionize cognitive warfare by enabling more sophisticated and effective strategies.

Nations should counter hybrid influence, especially in the cyber environment. States should ensure that activities in cyberspace and national policies are designed and implemented to support a compre-

hensive and systemic approach to cybersecurity and cyber defence. They should improve dialogue, cooperation and information exchange about national, regional and global cybersecurity. Building societal resilience against hybrid threats and cognitive warfare operations requires cooperation between all relevant civil society organizations, the private sector, academic communities and NGOs. Finally, extensive and interdisciplinary research, education and training are needed in cyberspace and the cognitive environment.



ENDNOTES

- [1] Martti Lehto and Gerhard Henselmann, 'Non-kinetic Warfare: The new game changer in the battle space', 15th International Conference on Cyber Warfare and Security, 2020, Old Dominion University, Norfolk, Virginia, USA, 316–325.
- [2] Alonso Bernal, Cameron Carter, Ishpreet Singh, Kathy Cao, and Olivia Madreperla, 'Cognitive warfare: An attack on truth and thought', NATO and Johns Hopkins University report, Fall 2020.
- [3] EU parliament, 'Insights, Understanding the EU's approach to cyber diplomacy and cyber defence', European Union, May 28, 2020, [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2020\)651937](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)651937).
- [4] Annegret Bendiek and Matthias C. Kettemann, 'Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy', SWP comment, no. 16, February 24, 2021, <https://www.swp-berlin.org/10.18449/2021C16/>.
- [5] Cyber Risk GmbH, 'The Cyber Diplomacy Toolbox', <https://www.cyber-diplomacy-toolbox.com/>.
- [6] NATO Cyber Defence, Factsheet, April 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf.
- [7] NATO, 'Cyber defence', last updated: 14 September, 2023, https://www.nato.int/cps/en/natohq/topics_78170.htm.
- [8] Julia Voo, Irfan Hemani, and Daniel Cassidy, 'National Cyber Power Index 2022', Harvard Kennedy School, Belfer Center Report, September 2022, <https://www.belfercenter.org/publication/national-cyber-power-index-2022>.
- [9] Chris Jaikaran, 'Cybersecurity: Deterrence Policy', 18 January, 2022, <https://csreports.congress.gov/product/pdf/R/R47011>.
- [10] Martti Lehto, 'Cyber-attacks Against Critical Infrastructure', in Cyber Security: Critical Infrastructure Protection, in Computation Methods in Applied Sciences series, ed. M Lehto and P Neittaanmäki (Springer 2022), 3–42, ISBN: 978-3-030-91293-2.
- [11] Anne Gardenier, Rinie van Est, and Lambèr Royakkers, 'Technological Citizenship in Times of Digitization: An Integrative Framework', Digital Society, Volume 3, Issue 2: 21 (2024), <https://doi.org/10.1007/s44206-024-00106-1>.
- [12] EU, 'Europe's Digital Decade: Digital targets for 2030', https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.
- [13] European Commission, 'Second report on the State of the Digital Decade calls for strengthened collective action to propel the EU's digital transformation', 02 July, 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3602.
- [14] Steve Morgan, 'Cybercrime to Cost the World \$10.5 Trillion Annually by 2025' (Special Report, 13 November, 2020), Cybercrime Magazine, <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>.
- [15] ENISA, 'Cybersecurity as an Economic Enabler', March 2016, <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler>.
- [16] Martti Lehto, 'Cyber-attacks Against Critical Infrastructure', in Cyber Security: Critical Infrastructure Protection, in Computation Methods in Applied Sciences series, ed. M. Lehto and P. Neittaanmäki (Springer 2022), 3–42, ISBN: 978-3-030-91293-2.
- [17] NATO, https://www.nato.int/cps/en/natohq/official_texts_227678.htm.
- [18] Arsalan Bilal, 'Russia's hybrid war against the West', NATO Review, 26 April, 2024, <https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html>.
- [19] Martti J. Kari, 'Russian Strategic Culture in Cyberspace', JYU Dissertations 122, 11 October, 2019.
- [20] Alexander Stubb, 'Comprehensive Security in the 21st century: The Finnish model', 08 May, 2024, <https://www.presidentti.fi/en/speech-by-president-of-the-republic-of-finland-alexander-stubb-at-hertie-school-in-berlin-on-8-may-2024/>.
- [21] Arsalan Bilal, 'Hybrid Warfare: New Threats, Complexity, and "Trust" as the Antidote', NATO Review, 30 November, 2021, <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>.
- [22] Stéphane Duguin and Pavlina Pavlova, 'The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict', EU Directorate-General for External Policies Policy Department, Workshop September 2023, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI\(2023\)702594_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf).
- [23] NATO, 'Speech by NATO Secretary General Jens Stoltenberg at event hosted by the NATO Association of Canada and the Canadian NATO Parliamentary Association', 19 June, 2024, https://www.nato.int/cps/en/natohq/opinions_226837.htm.
- [24] ODNI, 'Annual Threat Assessment of the U.S. Intelligence Community', 05 February, 2024, <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>.
- [25] Stéphane Duguin and Pavlina Pavlova, 'The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict', EU Directorate-General for External Policies Policy Department, Workshop September 2023, [https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI\(2023\)702594_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf).
- [26] CyberPeace Institute, <https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline>.
- [27] CSIS, 'Significant Cyber Incidents', <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.
- [28] DoS, 'GEC Special Report: August 2020 Pillars of Russia's Disinformation and Propaganda Ecosystem', August 2020.
- [29] Government of Canada, 'Russia's use of disinformation and information manipulation', 28 February, 2024, https://www.international.gc.ca/world-monde/issues_developpement-enjeux_developpement/reponse_conflict-reponse_conflits/crisis-crisis/ukraine-disinfo-desinfo.aspx?lang=eng.
- [30] NATO STRATCOM COE, 'Russia's Strategy in Cyberspace', June 2021.
- [31] Helmi Pillai, 'Protecting Europe's critical infrastructure from Russian hybrid threats' (Centre for European Reform, Policy Brief, 25 April, 2023), <https://mailings.cer.eu/publications/archive/policy-brief/2023/protecting-europes-critical-infrastructure-russian-hybrid-FN-25>.
- [32] Tim Maurer and Arthur Nelson, 'The Global Cyber Threat' (IMF report, Spring 2021), <https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm>.
- [33] Martti Lehto, 'Cyber-attacks against Critical Infrastructure', in Cyber Security: Critical Infrastructure Protection, in Computation Methods in Applied Sciences series, ed. M. Lehto and P. Neittaanmäki (Springer 2022), 3–42, ISBN: 978-3-030-91293-2.
- [34] Cyber National Mission Force, 'Before the Invasion: Hunt Forward Operations in Ukraine', 28 November, 2022, <https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/>.
- [35] Anthony Deutsch, Stephanie van den Berg and James Pearson, 'ICC probes cyberattacks in Ukraine as possible war crimes', 14 June, 2024, <https://www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14/>.

AUTHOR:

Dr Martti Lehto (Military Sciences), Col. (GS) (ret.) works as a Research Director at the University of Jyväskylä in the Faculty of Information Technology. His research areas are cybersecurity and cyberwarfare. He served for 30 years in the Finnish Air Force as a developer and leader of C4ISR Systems. He is also an adjunct professor at the National Defence University in air and cyberwarfare. He has more than 200 publications, research reports and articles on areas of cyber policy, cyberwarfare, cybersecurity education and critical infrastructure protection. The views contained in this article are the author's alone and do not represent the views of the University of Jyväskylä.



MARTTI LEHTO



PETER B.M.J. PIJPERS

Legislation as an instrument of cognitive warfare

Abstract:

Although subduing the opponent's will has been the pinnacle of warfare since Sun Tzu, the existing notion of cognitive warfare has gained traction with the possibility of influencing the opponent directly via cyberspace and social media. Influence operations via cyberspace entail swaying public opinion, manipulative psychological warfare, and lawfare. The use of law as an instrument of power to affect perception and cognition is possible because of ongoing legal disputes about how to apply (international) law to cyberspace. States can cherry-pick or even assertively exploit variations in interpretations of international law to pursue or defend their national interests as a means of cognitive warfare.

Problem statement:

Can states use legal ambiguity as an instrument of power to further their national interests?

Bottom line upfront:

The inception of cyberspace has invigorated existing influence operations. Cognitive influencing, or even warfare, uses digital means to saturate the veins of so-

cieties not only with narratives and propaganda but by weaponizing the varying interpretations of international law applicable to cyberspace to outmanoeuvre an opponent and further one's national interests.



So what?

Legislation is exploited to affect the cognition of target audiences. To tackle this, states first need to raise awareness about cognitive influencing and align their NATO/EU position against these aggressors. We must recognize that technological developments outpace legal absorptive capacity. However, we should be cognizant that law is used as an instrument of power. New laws must not reinforce authoritarian practices, but nor should they accentuate Western dominance.



Influence the will: An introduction

In May 2024 Annalena Baerbock, German Federal Minister for Foreign Affairs, attributed a cyberattack on the German Social Democratic Party (SPD) to APT 28, an agent of the GRU, the Russian Military Intelligence Service.[1] The attack, probably a spear-phishing attack, was part of a broader campaign to undermine the June 2024 European (EU) elections. Similarly, NATO's North Atlantic Council expressed concerns as it witnessed subversive and undermining cyberattacks against the Baltic states, Poland and the United Kingdom.

Elections are precarious periods for democracies; they are conceptual seams where a society moves from one set of elected lawmakers to another. In any system, whether organizing a military campaign or welding a heating system, seams are vulnerable. Liberal democracies are more vulnerable – as there are more seams in a democratic system – than authoritarian states, where there is often no genuine division, let alone a change, of power.

Influencing the people's will through elections was long part of the game plan in the bipolar Cold War. The Soviet Active Measures and American Political Warfare covered election interference to persuade or manipulate the cognition of foreign audiences and political leaders to elect or put in place a government in line with Soviet or US interests respectively.

Although subduing the opponent's will has been the pinnacle of warfare since Sun Tzu, the notion of cognitive warfare has gained traction with the growth of cyberspace and the possibility of influencing opposing audiences directly via social media. Cyberspace is a human-made domain that has added three layers to the existing information environment: the hardware itself; the virtual persona we use to communicate online; and the data and protocols that make communication possible.[2]

These additional layers provide new target surfaces that state and non-state actors will want to protect or use to engage with others.

The dawn of cyberspace has enabled three cyber-related categories of activities: digital intelligence gathering (espionage) through scanning or copying of data confined to virtual repositories; subversive digital influence operations;[3] and digital undermining.[4] The latter cyberattacks are activities in the virtual dimension that undermine cyberspace with binary code, modify or manipulate data, and degrade or destroy the hardware or protocols, resulting in virtual and/or physical effects in cyberspace. Digital influence operations use cyberspace as a vector (without affecting it) to target the (human) cognitive dimension of groups or audiences, using content, words, memes and footage as “weapons”. [5] Apart from large state-supported activities such as Stuxnet in the past, most cyberattacks witnessed in Ukraine and Gaza have had a limited impact. Conversely, state-level influence operations, including Russian interference during the 2016 US presidential election, did have strategic effects.[6]

Apart from activities in cyberspace, the wars in Ukraine and Gaza have witnessed the emergence of new actors and technologies. Non-state actors, including Anonymous, Microsoft and Elon Musk, play a role in these conflicts without becoming a belligerent party, and artificial intelligence is used in targeting systems in the Gaza war.[7] These topics raise not only operational and ethical but also legal questions – for example, concerning DDoS attacks by a non-state actor and international humanitarian law (IHL), or IHL article 49 AP1's coverage of cyberattacks.[8]

Using or exploiting states' varying interpretations of (international) law can even be used as an instrument of power to affect perception and cognition. This form of “lawfare”[9] can be a tool for influencing the cognition of target audiences through cyberspace. States can cher-

ry-pick or assertively exploit the variations in interpretations of international law to pursue or defend their national interests as a means of cognitive warfare.

What is cognitive warfare?

From a security or military perspective the cognitive domain is the pinnacle of warfare. Thinkers such as Thucydides and von Clausewitz argue that the essence of warfare is to subdue an enemy – ensuring that the opposing actor (willingly or unwillingly) becomes convinced that it should change its behaviour and act in accordance with our will.

In the past the cognitive domain was influenced by physical acts and therefore indirectly by the (threat of the) destruction of armies or capitals. With the inception of cyberspace and the increased knowledge of cognitive psychology,[10] today's cognitive warfare also directly targets the mind, using influence and information operations and psychological warfare – hence, warfare without the use of kinetic force. Cognitive activities can be applied to persuade our conscious mind. However, their focus is on exploiting our subconscious mind,[11] the main driver of our behaviour: biases; heuristics; intuition; and emotions.

As a conceptual notion cognitive warfare cannot easily be defined. In a research paper by Cluzel it is compared to hacking the minds of individuals to “erode the trust that underpins every society”, which includes the use of neuroscience and technology.[12] Hung and Hung argue that information warfare is a subset of cognitive warfare,[13] and influence operations are merely the cyber-related elements of information warfare. Others argue the opposite, stating that “cognitive warfare has absorbed information warfare”. [14] In both cases there is a shift from controlling the media (information) to controlling the brain (cognition).

NATO's proposed definition is “deliberate, synchronised military

and non-military activities throughout the continuum of competition designed to affect audience attitudes, perceptions and behaviours to gain, maintain and protect cognitive superiority”.[15] Other definitions of cognitive warfare argue that it is a strategy that focuses on altering how a target population thinks, and thus how it acts. Alternatively, they claim that “in cognitive warfare, the ultimate aim is to alter our perception of reality and deceive the brain in order to affect our decision-making”.[16] In all definitions and descriptions of cognitive war, trust and truth are the primary targets.[17]

Cognitive warfare via cyberspace

With the growth of cyberspace our societies have become more digitalized, but warfare is also digitalized. The potential and actual impact of cyberactivities is widely debated. Although some scholars argue that cyberwarfare equates to regular warfare, a more common view is that most cyberoperations will not reach the threshold of war. This means that labelling cyberoperations will benefit from examining the effects they may have rather than the act itself.[18]

A recent example of large-scale cyberactivities is the Russia–Ukraine war. There have been more than 3,500 attacks since the start of the invasion in February 2022.[19] Various actors, including states, have undertaken these attacks. However, 95 per cent can be labelled as DDoS, defacements, or hack (and leak) operations, and some 90 per cent of these were executed by non-state actors. DDoS and defacements are what Gartzke and Lindsay categorize as hindrances or nuisances,[20] neither causing “death and destruction” nor directly supporting a military campaign. Although some cyberattacks have supported operational-level military or diplomatic campaigns, including digital espionage or severe wiperware attacks, none with a severe strategic impact (similar to a cyber Pearl Harbour) has been registered.

Despite the scale, the impact of cyberspace activities in the Russia–Ukraine war appears marginal, possibly due to Ukrainian resistance, resilience (supported by firms such as Microsoft) and faltering Russian operations. There are some notable exceptions, however, as some cyberoperations have served their purpose. First, on the eve of the invasion Russia attacked the “Viasat” satellite internet connection, imposing a digital blackout on Ukrainian forces. Second, Ukrainian president Zelenskyy’s fervent online strategic communication with foreign parliaments has resulted in diplomatic support and the supply of funds, military systems and ammunition.

Contrary to undermining cyberattacks, digital influence operations can have strategic effects. While influence operations are not inherently malign, they intend to affect deliberate understanding and autonomous decision-making processes of humans or groups consciously, or preferably, subconsciously. Ultimately, cognitive warfare via influence operations in cyberspace does not aim for the destruction of humans but the “reformatting” of the target audience with values, morality, and an understanding of good and evil in line with the wishes of the attackers.[21]

Since the annexation of Crimea pro-Russian state and non-state actors have conducted cyber-enabled disruptive propaganda and disinformation campaigns to create an information environment with opposing views and perceptions.[22] The main purpose of Russian “information confrontation”[23] operations is to demoralize the Ukrainian population and drive a wedge between Ukraine and its Western allies. Influence operations are also used to target domestic Russian audiences. The narratives used are Western Russophobia, the “denazification and demilitarization” of Ukraine, and the endemic corruption within the Ukrainian government.[24] Ukraine similarly exploits social media. Since the invasion President Zelenskyy has addressed his population on-

line and maintained the morale of his troops, positively affecting the cognitive dimension of both friend and foe.[25] International support is Ukraine’s lifeline and is thus both a centre of gravity and therefore also an Achilles’ heel.[26]

Influence operations, especially manipulative ones, are inherently deceptive and use heuristics and biases, luring the target audience away from a rational decision-making process in favour of what Petty and Cacioppo call the peripheral route.[27] The peripheral route is invoked by using a socially divisive topic to distract a targeted audience, impairing their ability to process incoming data due to the emotional or provocative sentiment attached. Hung and Hung make a similar assessment, arguing that cognitive warfare uses two dimensions: psychological techniques (how our brain works) based on heuristics and repeated stimulation; and the cognitive handling of external information. To influence humans, a gap (or “free energy”) needs to exist – or to be created – between prior predictions and incoming stimuli; in effect, the target audience needs to start to doubt, which is in line with the Russian information confrontation approach.[28]

Western democracies are more vulnerable to manipulative influence operations as an element of cognitive warfare – and hence to Russian information confrontation – because of their open societies built on the freedom of speech, the press, and to vote and be elected. Notions embedded in the principles of legality and legitimacy go hand in hand with the trust people have in the government, judges, and traditional (often written) media. Western democracies are entirely free to discuss and absorb incoming stimuli, create new ideas, innovate, fail, and learn. This contrasts with authoritarian states, which attempt to undermine incoming (foreign) stimuli, information and new ideas to ensure the population’s inoculated perception (or prior beliefs) is aligned with the (state-controlled) information envi-

ronment and not distorted by (false or factual) evidence that will change the prior belief and create doubt.

Legislation in cognitive warfare

Alongside the example of Russia's information confrontation the Chinese Three Warfares is another example of cognitive warfare. This doctrine, governed mainly by the Chinese Communist Party's (CCP) United Front Work Department[29] and the People's Liberation Army,[30] aims to maintain the CCP's political power and "control the prevailing discourse and influence perceptions to advance China's interest".[31] To suppress incoming stimuli and propagate a benign image of the People's Republic of China (PRC), diasporas are dissuaded from voicing dissenting opinions. The internet and social media are frequently censored domestically.[32] The Three Warfares doctrine not only entails a persuasive and manipulative perception but also a legal one of how to change the attitude and thus the behaviour of targeted audiences – at home or abroad.[33]

Persuasive public opinion warfare, or media warfare, aims to shape "targeted audiences through information derived and propagated by mass information channels", both traditional (television, newspaper, movies) and on the internet.[34] Public opinion warfare is related to shaping (online) public opinion to transmit a consistent message to the targeted audience in a way favourable to Chinese positions.[35]

Whereas public opinion warfare focuses on framing or highlighting some aspects of the truth while neglecting others, often with a pinch of humour, psychological warfare is more manipulative. Psychological warfare involves using information to pressure an opponent and "create damaging or deleterious habits and ways of thinking, to reduce its will to resist, and perhaps even to induce defeatism and surrender".[36] Psy-

chological warfare uses a variety of techniques, including intimidation, religious interference,[37] dissuasion, manipulation and deception.[38]

Interestingly, the Chinese Three Warfares are applicable in all conflict phases (from peace to war), using diverging legal interpretations to influence others. Legal warfare is designed "to justify a course of action"[39] forging a normative environment favourable to China. The PRC's legal warfare, which echoes Western debates on lawfare,[40] is a tool of non-kinetic warfare that offers influence on an actor's behaviour to achieve strategic ends. Successful legal warfare limits others' freedom of movement while expanding the PRC's freedom of action.[41]

Three Warfares is not a specific policy of the CCP. Its effectiveness is that it is a society-wide endeavour. When addressing foreign audiences, the Three Warfares activities use the PRC's entire media landscape so that different sources and versions reiterate and reinforce a given message. Outlets include media channels (CGTN), cultural institutes (Confucius Institutes), Chinese exchange students,[42] diaspora communities, think tanks and the Chinese diplomatic network to affect foreign audiences.[43]

Law as an instrument of warfare

The PRC's legal warfare exploits the ambiguity in international law related to new developments, a discourse that is not new. Nuclear weapons and aeroplanes were introduced after the Laws of Armed Conflict (IHL) were conceived. However, as (international) law is based on principles including military advantage, distinction, proportionality and necessity, not on specific situations or techniques, the law will still apply. In practice a discourse will start on how to apply the existing international law to the new development – for example, in the United Nations Group of Governmental Experts or the Open-Ended Working Group.[44]

On the one hand, as international law is based on principles from which rules are derived, it has always been the purpose of the body of international law to provide legal room to manoeuvre so that generic rules can be applied to a specific situation or new developments.[45] On the other, new developments can cause challenges, not least due to the speed of (technological) developments, including artificial intelligence,[46] human enhancement, drones and cyberspace. This parallax causes uncertainty about how to apply the law. There is a debate in cyberspace about whether sovereignty – a legal obligation in traditional international law – is a rule (obligation) and principle or merely a principle of law; the latter is the UK position. This is not a semantic discussion because if sovereignty is a principle – and hence not an obligation – it cannot be violated. The articles on State Responsibility state that an Internationally Wrongful Act constitutes a breach of a primary rule of law (an obligation) that can be attributed to a state. If sovereignty is breached by a state that does not see it as an obligation, the redress or countermeasure may be a violation of international law, in which case a row could escalate into a conflict.

Another source of ambiguity is whether cyberspace is itself part of the territory of a state and thus subject to its laws. In many Western views territory includes the soil, the territorial sea and the air column above them, not space in general or the virtual aspects of cyberspace – the zeros and ones.[47] In this sense cyberspace's virtual dimension is borderless. In many authoritarian states the totality of cyberspace is linked to the control of territorial integrity. Hence, the PRC argues that it has digital sovereignty over cyberspace "on its soil", while Western states only have territorial control of the hardware on their soil.

Moreover, while Western states argue that international law supercedes national law, the Russian constitution argues that national law has

priority over international law. Conversely, the PRC uses international law to underline its claims in the South China Sea, for example,[48] and disputes the Western view that only natural (not artificial) islands are part of a territorial claim.

Finally, there is no clear distinction for the PCP between war and peace. Based on the Three Warfares, these forms of “warfare” commence before any actual military engagement and are conducted to shape and prepare the battlefield and its participants. All these forms of the Three Warfares are applicable across the spectrum of war and peace.

How to counter the use of lawfare

The use of law as an instrument of power to affect perception and cognition is possible because of ongoing legal disputes, and states hold varying interpretations about how to apply (international) law to cyberspace. To counter the activities of cognitive warfare effectively, it is critical to understand the aggressor’s intent before responding. NATO and EU states must raise public awareness of possible foreign cognitive warfare activities, including lawfare, and align common positions within the alliances. Finally, a discourse on whether new law is required remains valid.

First, states, especially liberal democracies, must understand that Chinese and Russian cognitive warfare differ in intent and depth. Russian activities are intended to sow confusion through the dissemination of information that conflicts with or confronts existing knowledge. An example of this is the firehose of falsehoods that followed Russia’s downing of MH17. Russian cognitive and influence operations can be seen as a blunt instrument affecting audiences in foreign states, with no other intention than to confuse, sow discord and undermine trust in democratic foundations. Although Russia exploits the variances of international law, it would prefer to neglect it altogether.

Conversely, Chinese activities are subtle and clearly intend to uphold or improve foreign audiences’ benign image of the PRC. The PRC relies on international law but favours a renegotiation of its foundations because, according to the PRC, the current body of international law is a reflection of Western interests. In countering the cognitive activities of Russia or the PRC, the intent of the aggressor needs to be considered. The worst mistake would be to assess the cognitive act in accordance with Western standards.

Raising awareness is (generally) an effective means to counter cognitive warfare. US citizens were unaware of the impact foreign actors’ social media campaigns could have in the run-up to the 2016 presidential election – a naivety that had already largely vanished by the 2018 mid-term elections. Free access to education is pivotal, as are educational programmes for schools on the advantages and dangers of an open and free (and hence unfiltered) internet where this is already the case.

Besides raising awareness, coalition alignment can also block foreign cognitive warfare by formulating a common position and forming a common bloc among NATO/EU member states with partners such as Japan and Australia. Adversaries will exploit the seams in these coalitions, especially when there is no com-

mon rationale, as we currently see in the fragile alignment and hence increased friction within the varying positions of NATO/EU member states regarding the Ukraine war.[49]

Most international legal scholars argue that the current law is sufficient. Yet refinement is needed concerning how to apply the law, for which more state practice and legal statements (*opinio iuris*) by states are needed. There is a danger that this is wishful thinking. It will be a real challenge to align the diverging opinions of states – as sound legal opinions or as a reflection of political pragmatism. Some states are already entrenched or have seen the benefits of using law as an instrument of power during UN/OEWG sessions, for example.

Moreover, new developments (AI, quantum computing) are more complex than in the past, and international law can no longer keep pace with new developments. EU lawmakers remain unable fully to grasp the potential and danger of developments such as AI. They correctly see the need for legislation, however. The result is laws that above all reflect the consensus building of the legislative process, but that are highly ambiguous in content, in turn fuelling legal cherry-picking and hence the use of law as an instrument of power – a devil’s dilemma.



ENDNOTES

- [1] APT means an advanced persistent threat (usually a state (financed) cyber actor); the GRU is the Russian military intelligence service. See Marcel Rosenbach and Christophe Schult, 'Baerbocks Digitaldetektive decken russische Lügenkampagne auf', *Der Spiegel*, 26 January, 2024, <https://archive.ph/2024.01.26-114242/https://www.spiegel.de/politik/deutschland/desinformation-aus-russland-auswaertiges-amt-deckt-pro-russische-kampagne-auf-a-765bb30e-8f76-4606-b7ab-8fb9287a6948>.
- [2] Peter B.M.J. Pijpers, 'Careful what You Wish for: Tackling Legal Uncertainty in Cyberspace', *Nordic Journal of International Law* Volume 92, Issue 3 (2023): 397–399.
- [3] Andreas Krieg, *Subversion: The Strategic Weaponization of Narratives*, 2023.
- [4] Peter B.M.J. Pijpers and Kraesten L. Arnold, 'Conquering the Invisible Battleground', *Atlantisch Perspectief* Volume 44, Issue 4 (2020): 11–14; Paul A.L. Duchaine, Peter B.M.J. Pijpers, and Kraesten L. Arnold, 'The "Next" War Should Have Been Fought in Cyberspace, Right?', in *Beyond Ukraine, Debating the Future of War*, eds Tim Sweijs and Jeff Michaels (Hurst Publishers, 2024); Paul A.L. Duchaine, Jelle van Haaster, and Richard van Harskamp, 'Manoeuvring and Generating Effects in the Information Environment', in *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crisis – NL ARMS 2017*, ed. Paul A.L. Duchaine and Frans P.B. Osinga, 2017.
- [5] Miranda Lupion, 'The Gray War of Our Time: Information Warfare and the Kremlin's Weaponization of Russian-Language Digital News', *Journal of Slavic Military Studies*, Volume 31, Issue 3 (2018): 329–330; Calder Walton, 'What's Old Is New Again: Cold War Lessons for Countering Disinformation', *Texas National Security Review*, Fall 2022.
- [6] Ellen Nakashima, 'Pentagon Launches First Cyber Operation to Deter Russian Interference in Midterm Elections', *The Washington Post*, 2018, https://www.washingtonpost.com/world/national-security/pentagon-launches-first-cyber-operation-to-deter-russian-interference-in-midterm-elections/2018/10/23/12ec6e7e-d6df-11e8-83a2-d1c3da28d6b6_story.html.
- [7] Yuval Abraham, '"Lavender": The AI Machine Directing Israel's Bombing Spree in Gaza', +972 Magazine, April (2024), <https://www.972mag.com/lavender-ai-israeli-army-gaza/>.
- [8] Article 49.1. of the 1977 Additional Protocol (1) to the Geneva Conventions states: "Attacks" means acts of violence against the adversary, whether in offence or in defence.
- [9] Orde F. Kittie, *Lawfare: Law as a Weapon of War*, (Oxford University Press, 2016), 4–8.
- [10] Francois du Cluzel, 'Cognitive Warfare' (Innovation Hub, 2021), 12.
- [11] Cornelus van der Klaauw, 'Cognitive Warfare', in: *The Three Swords* Volume 39 (2023), 99.
- [12] Francois du Cluzel, 'Cognitive Warfare', 7.
- [13] Tzu-chieh Hung and Tzu-wei Hung, 'How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars', *Journal of Global Security Studies* Volume 7, Issue 4 (2020): 2–4.
- [14] Russtrat, 'Cognitive Warfare: War of a New Generation', Institute of Russian Strategies, 24 December 2021, https://russtrat.ru/en/analytics_/24-december-2021-2228-7813.
- [15] NATO Cognitive Warfare Concept, version of 17 April 2024, Supreme Allied Command Transformation.
- [16] Cornelus van der Klaauw, 'Cognitive Warfare', 100.
- [17] Alonso Bernal et al., 'Cognitive Warfare: An Attack on Truth and Thought', NATO & John Hopkins, 2020; Francois du Cluzel, 'Cognitive Warfare', (Innovation Hub, 2021), 8–9.
- [18] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., (Cambridge University Press, 2017).
- [19] CyberPeaceInstitute, 'Cyber Dimensions of the Armed Conflict in Ukraine' (2023), <https://cyberconflicts.cyberpeaceinstitute.org>.
- [20] Jon Lindsay and Erik Gartzke, 'Coercion through Cyberspace: The Stability-Instability Paradox Revisited', in *The Power to Hurt: Coercion in Theory and in Practice*, 2016, 179–203.
- [21] Russtrat, 'Cognitive Warfare: War of a New Generation'.
- [22] Todd C. Helmus et al., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Rand Corporation, 2018), 7–25.
- [23] Michelle Grisé et al., *Russian and Ukrainian Perspectives on the Concept of Information Confrontation*, Rand Research Report, 2022, 5–10.
- [24] Tine Molendijk, 'Morale and Moral Injury among Russian and Ukrainian Combatants', in *Reflections on the Russian-Ukrainian War*, eds Maarten Rothman, Lonneke Peperkamp, and Sebastiaan Rietjens, (Leiden University Press, 2024), 99–106.
- [25] The story of a Ukrainian fighter pilot, 'the Ghost of Kyiv', went viral online. Another occurrence concerned the bold response of Ukrainian troops defending Snake Island after Russia's Black Sea Fleet flagship 'The Moskva' demanded their surrender or the attack on the Kerch bridge.
- [26] Paul A.L. Duchaine, Peter B.M.J. Pijpers, and Kraesten L. Arnold, 'The "Next" War Should Have Been Fought in Cyberspace, Right?', 101–104.
- [27] Richard E. Petty and John T. Cacioppo, 'The Elaboration Likelihood Model of Persuasion', *Advances in Experimental Social Psychology* 19 (1986): 126.
- [28] T.S. Allen and A.J. Moore, 'Victory without Casualties: Russia's Information Operations' Parameters Volume 48, Issue 1 (2018): 60.
- [29] Marcel Anglivièl de la Beaumelle, 'The United Front Work Department: "Magic Weapon" at Home and Abroad', *China Brief* Volume 17, Issue 9 (2017).
- [30] But not solely: the ministry of State Security, the Taiwan Affairs office and the Central Committee of the Party (international liaisons, propaganda and the United Front work department) are involved, to name only a few.
- [31] Pieter Zhao, 'Chinese Political Warfare: A Strategic Tautology? The Three Warfares and the Centrality of Political Warfare within Chinese Strategy', *The Strategy Bridge*, August (2023), <https://thestrategybridge.org/the-bridge/2023/8/28/chinese-political-warfare-a-strategic-tautology>.
- [32] Alina Polyakova and Chris Meserole, 'Exporting Digital Authoritarianism: The Russian and Chinese Models', Policy Brief, Democracy and Disorder Series, 2019, 1–22, 2–6.
- [33] Albert Zhang, 'Gaming Public Opinion Influence Operations', *ASPI Policy Brief* no. 71 (2023).
- [34] Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, Praeger, 2017, 51–53; Peter Mattis, 'China's "Three Warfares" in Perspective', in *War on the Rocks*, 2023.
- [35] See e.g.: CGTN Official, 'Samarland, Listed by UNESCO as a World Heritage Site', X (Twitter), 2023, <https://twitter.com/cgtnofficial/status/1707625764412440805?s=43&t=7ecH6cep1ONZNAMcRFBW>.
- [36] Deng Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations*, 44–45.
- [37] Tzu-chieh Hung and Tzu-wei Hung, 'How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars', 4.
- [38] Paul Charon and Jean-Baptiste Jeangène Vilmer, 'Chinese Influence Operations: A Machiavellian Moment', IRSEM, 49–51; Nadine Yousif, 'MP Michael Chong Urges US-Canada Cooperation on China Interference', *BBC News*, 2023, <https://www.bbc.com/news/world-us-canada-66791749>.
- [39] Emilio Iasiello, 'China's Three Warfares Strategy Mitigates Fallout from Cyber Espionage Activities', *Journal of Strategic Security* Volume 9, Issue 2 (2016): 56.
- [40] Aurel Sari, 'Hybrid Threats and the Law: Concepts, Trends and Implications', 2020, 10–12.; Bret Austin White, 'Reordering the Law for a China World Order: China's Legal Warfare Strategy in Outer Space and Cyberspace', *Journal of National Security Law & Policy* Volume 11, Issue 2 (2021): 435–88.
- [41] Charon and Jeangène Vilmer, 'Chinese Influence Operations: A Machiavellian Moment', 51–55.
- [42] Pieter Zhao, 'Chinese Political Warfare: A Strategic Tautology? The Three Warfares and the Centrality of Political Warfare within Chinese Strategy', *The Strategy Bridge*, August (2023), <https://thestrategybridge.org/the-bridge/2023/8/28/chinese-political-warfare-a-strategic-tautology>.
- [43] Rush Doshi and Robert D. Williams, 'Is China Interfering in American Politics?', *Lawfare*, October (2018).
- [44] United Nations General Assembly, 'Final Substantive Report', Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021.
- [45] See e.g. the so-called Martens Clause in the preamble of the 1899 Hague Convention of the Law and Customs of War on Land.
- [46] Todd C. Helmus, 'Artificial Intelligence, Deepfakes, and Disinformation: A Primer', *Rand Perspective*, July (2022); Adrian Agenjo, 'Lavender Unveiled: The Oblivion of Human Dignity in Israel's War Policy on Gaza', *Opinio Juris*, April (2024): 1–5, <http://opiniojuris.org/2024/04/12/lavender-unveiled-the-oblivion-of-human-dignity-in-israels-war-policy-on-gaza/>.
- [47] Michael N. Schmitt, 'Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations', *International Review of the Red Cross* (Cambridge University Press, 1 April 2019).
- [48] National Institute for South China Sea Studies, 'A Legal Critique of the Award of the Arbitral Tribunal in the Matter of the South China Sea Arbitration', *Asian Yearbook of International Law* 24 (2020).
- [49] Vladimir Soldatkin and Anita Komuves, 'Hungary's Orban talks Ukraine peace with Putin, stirring EU outcry', *Reuters*, <https://www.reuters.com/world/europe/hungarys-orban-says-no-position-negotiate-between-ukraine-russia-2024-07-05/>.

AUTHOR:

Dr Peter B.M.J. Pijpers is an associate professor of cyber operations at the Netherlands Defence Academy, a researcher at the University of Amsterdam Centre for International Law, and a non-resident fellow at the University of South Florida Global and National Security Institute. Dr Pijpers has published on the legal and cognitive dimensions of influence operations in cyberspace, and how armed forces can manoeuvre in the information environment. See also Orcid ID 0000-0001-9863-5618. The author can be contacted at b.m.j.pijpers@uva.nl. The views contained in this article are the author's alone and do not represent those of the Netherlands Defence Academy.



PETER B.M.J. PIJPERS

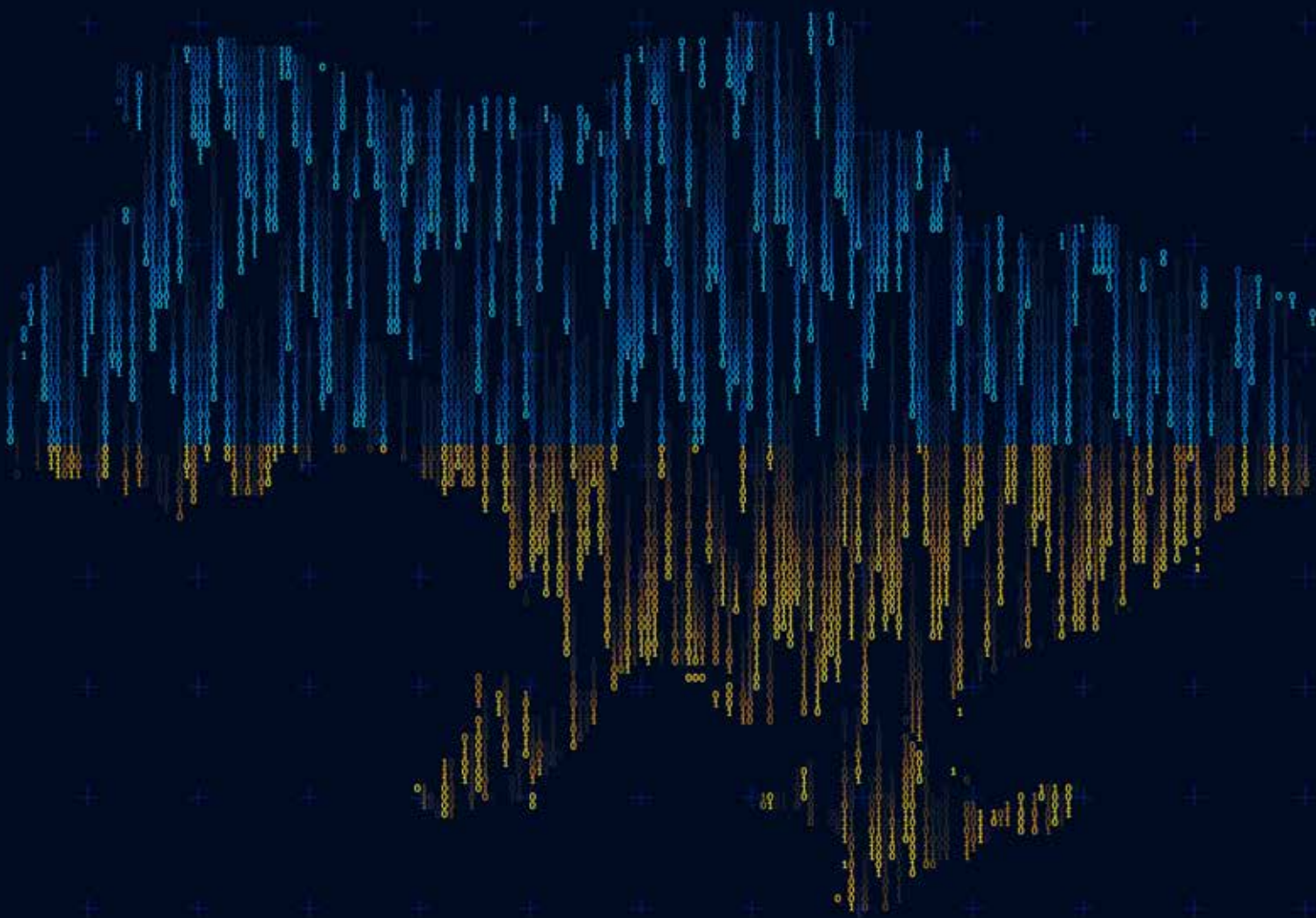


Cyberwatch Finland

WEEKLY REVIEW

9/2025

War in Ukraine special



Cybersecurity is Built by Small Actions and Management of Large Concepts



Foreword

On Monday it became three years since the start Russia's of the large-scale invasion of the war in Ukraine. To commemorate the anniversary, Cyberwatch Finland publishes a weekly review on the cyber dimension of the war in Ukraine. In the early stages of the large-scale invasion, the war in Ukraine was commented on as the world's first unrestricted cyber war, and the cyber component was viewed with curiosity and a lot

of hope was placed on it. Since then, the understanding of the purposes of cyber warfare has become more precise, and cyber warfare has evolved. It has also had a wide-ranging impact on the European and Western security environment. What the fourth year of the invasion or possible peace negotiations will mean in the cyber environment is currently unknown, but educated estimates can nevertheless be made.

The evolution of cyber warfare

The background to Ukraine's cyber war should be sought further than the launch of a large-scale attack in February 2022. Actually, the war itself can be counted as having already started with the annexation of Crimea in 2014 and the events in Eastern Ukraine. The years 2014–2022 paved the way for a large-scale invasion also in the cyber world. For example, online dis- and misinformation and other forms of cognitive warfare were visible in Ukraine, Europe and Russia.

Between 2014 and 2022, Ukraine faced some cyberattacks. One of the most notable was a cyberattack on the country's electricity grid in 2015, which left more than 200,000 residents without electricity for several hours. The electricity grid was attacked again with a cyberattack in 2016, when hundreds of thousands of people were left without electricity in the capital Kyiv, in the middle of the winter frosts. However, the effects of latter attack were limited to only about an hour. In 2017, Ukraine was plagued by Pet-ya ransomware attacks, which have since been linked to Russia by the CIA and Ukrainian authorities. The time before the large-scale invasion was also used to infiltrate Ukraine's critical systems for later use. In January 2022, Ukraine was hit by cyberattacks, which were probably aimed to cause fear and disorder and thus pave the way for the large-scale attack at the end of February.

Russia's cyber activities after a large-scale invasion have typically been described as three-phased. In the first phase, Russia quickly triggered the footholds it had previously gained in Ukrainian systems. This includes cyberattacks that have affected critical infrastructure and communications, such as hacking of Viasat satellites and attacks on Ukrainian organisations with the intention of destroying everything possible with wiper-malwares. However, cyberattacks did not succeed in permanently destroying systems or critical infrastructure and very soon, Russia realised that it was probably easier and faster to destroy infrastructure through traditional kinetic influenc-

ing. This led to a switch, where Russia started to focus more on cyber intelligence and information theft in cyberattacks. The aim was to collect information on the damage caused by physical attacks and other strategic targets. In the third phase, the form has been some kind of compromise between the two previous, in which attacks are carried out, but more precisely and deliberately.

From the Ukrainian side different phases are not as clearly distinguishable. Prior to the large-scale attack, the importance of international cooperation, especially the US Hunt Forward operation, which began in December 2021, has been emphasised in strengthening cyber defence. With regard to offensive cyber power, Ukraine was able to mobilise quite a large number of volunteers to support its own cyber activities at the beginning of the attack, and for example instructions on how to carry out denial-of-service attacks were widely distributed. Over the years, the number of cyberattacks carried out by Ukraine has continued, and volunteers have been increasingly tied up as part of the structures of the military. Ukraine's most visible cyberattacks on Russia have been cyberattacks on state authorities and various registers. At the same time, efforts have been made to strengthen Ukraine's cyber defence with the help of international support.

Perhaps the most surprising thing is that so far, the cyber war in Ukraine hasn't had such a significant effect or development which was imagined in the early weeks of large-scale invasion. These were expected, for example, in the form of completely new attack methods, malware or other technical cyber innovations. It is possible that the most significant innovations are kept as secrets and efforts are made to prevent their spread. Before the large-scale attack and even when it began, the role of the cyber environment was thought to be remarkably different from what it actually was. Russia could not bring Ukraine to its knees by cyber means, and the destructive power of cyber weapons turned out to be smaller than expected.

The current situation on the Ukrainian cyber front



The cyber operations of the war in Ukraine that are currently underway can be roughly divided into three categories. Attacks between Ukraine and Russia on each other's systems, Russian operations in countries supporting Ukraine, and information environment operations. As mentioned, the first category attacks were most active during the first year of the war, when Russia launched the weapons it had prepared and took advantage of the footholds it had gained. Since then, visible and publicized Russian attacks have been comparatively less frequent, as they focus on clandestine intelligence gathering.

At the moment, one sees more often news about Ukrainian attacks on Russian targets. The latest example is the attack on the Russian oil giant Gazprom at the end of January, in which the Ukrainians allegedly managed to paralyze the company's online services for a few days. The incident illustrates well why Ukraine carries out these attacks. Their goal is to make the war visible and tangible to ordinary Russians by influencing the services in use and gnawing at the narratives of the mainstream media about how well the special operation is going. The second goal is to maintain own and allies' fighting spirit by reporting on successes and reminding them that the struggle continues on all fronts. The January attack is an excellent example in this regard as well, as it was carried out on the same day as historic Battle of Kruty in 1918. The Battle of Kruty is a well-known symbolic event in Ukraine, in which a contingent of Ukrainian cadets successfully defended Kyiv against tenfold Russian superiority. Attempts are now being made to awaken a similar spirit through cyberattacks. Although Gazprom is unlikely to suffer any significant losses or adverse effects from the attack in reality, the goals of the attacks in Ukraine often lie elsewhere than directly influencing the operations of Russian companies. A significant part of cyber resources is likely to be directed to protecting against espionage and intelligence gathering operations, but the successes (or failures) that occur in this are often hidden from the public.

Of the cyber operations carried out by Russia, attacks on Ukraine's allies or supporters have received the most attention recently. These include both low-level denial-of-service attacks, which are carried out daily by various hacktivist groups, and operations by higher-level APT groups. The latter vary in their method of implementation and targets, but a clear change has taken place during the war in how many operations

are directed to Ukraine and how much outside it. During the first year of the war, the attention of Russian APT groups seemed to be almost exclusively on Ukraine, but during 2023 and especially 2024, Western countries were selected as targets several times. A concrete observation of this was made in April 2024, when an advanced malware called Kapeka, developed during the war in Ukraine, was detected across Europe. The reasons why the targets have been selected from outside Ukraine are that it is possible for Russia to use more direct weapons in Ukraine than covert cyber operations, and that the desired destructive effect was not achieved in Ukraine with an extensive cyber campaign.

A visible cyber phenomenon of the war in Ukraine has also been the struggle in the information environment. This has continued in a similar way practically throughout the war, with both sides trying to convince their own side of the success, as well as influencing the prevailing narratives in neutral countries by producing news and fake news that serve their own goals. In the early stages of the large-scale invasion, Ukraine's strategic message in particular was stronger, and turned public opinion in the West to its side. Russia, on the other hand, has had its own audience in Latin America and Africa, for example. Over the years, Ukraine's message has weakened, which can be seen in Europe as pain regarding aid to Ukraine and as an increase in opinions that understand Russia, for example in Germany.

In 2025, the most significant topic on which the parties spread different narratives has been the change of power in the United States and its impact on the future of the conflict. In the Russian media, Trump's rise to power has been seen as a positive factor that has a significant impact on Ukraine's ability to wage war. For example, in the headlines of the Russian magazine *Argumenty i fakty* (Аргументы и Факты), Trump is said to be plucking Ukraine clean and making statements accusing Zelensky of being an inept diplomat whose poor negotiation skills are the cause of the war in the first place. Ukraine's state media Ukrinform, on the other hand, rarely mentions Trump, and the news emphasizes the role of aid provided by parties other than the United States and tries to draw attention to the active events of the war and Ukraine's victories on the front instead of the international situation. In addition media on both sides is still full of almost daily news about success on the front, with both likely exaggerating their success.



Impact on the wider European cyber environment

The war in Ukraine has had a significant impact on the European and international cyber environment. The most visible impact has been the cyber attacks on Europe carried out by pro-Russian volunteer hacktivists. The most typical attacks have been denial-of-service attacks or distributed denial-of-service attacks. Defacement of websites with inappropriate content has also been seen. Hactivist campaigns received quite a lot of attention in the early stages of the large-scale war of aggression, but since then people have become accustomed to it and a certain "harmlessness" of the attacks has been recognized.

On the other hand, hybrid influencing has been of wider importance, which has also been carried out by cyber means, especially with regard to critical infrastructure. In Finland and Europe, companies in the critical infrastructure sector, such as Fingrid, which is responsible for electricity networks, and several telecommunications operators have reported attempts to break into systems in addition to daily denial-of-service attacks. So far, the protection has worked, and there have been no huge cyber disasters. It is possi-

ble that while Russia is destroying Ukraine's critical infrastructure in the form of missiles and other conventional weapons, cyber weapons against critical infrastructure have been saved for the West. Physical sabotage related to hybrid influencing is also increasing, which has been seen in the Baltic Sea region in the form of broken telecommunications cables, among other things.

At the same time, cyber espionage is believed to have increased in Europe. The travel restrictions imposed on Russians, the expulsion of diplomats and other measures that have narrowed the mobility of Russians in Europe have forced Russia to move more towards cyber intelligence. Although state-level operations are rarely discussed openly, even when they are revealed, some cyber operations carried out by Russian APT groups on European targets have ended up in the public domain during the war. Naturally Russia is not the only actor practicing cyber espionage in Europe, as, for example, China is also involved in the activity, and North Korea's interest in defense companies has also been reported.



Conclusion

The war in Ukraine is clearly entering a new phase with talks about possible peace negotiations. At the time of writing, it is difficult to say in which direction the development is heading. There are different views on whether a possible ceasefire and peace will accelerate or reduce cyber attacks. It is unlikely that in any scenario a cyber-attacks would cease completely. The direction in which the cyber front will develop is the sum of many factors, and it is difficult to predict the near future. Peace talks or a ceasefire may reduce the number of visible operations and provide a respite for the parties, but on the other hand, especially Russian provocations and testing of a ceasefire would be likely. The terms of a possible peace or truce are also likely to affect how willing the parties are to engage in cyber operations.

At the moment, it is important to monitor the progress of possible peace negotiations in Ukraine and their impact on the cyber environment. Depending on what the next few months bring, Russia may free up more cyber capacity for operations against Western countries. In addition, it should be noted that probably the best lessons learned from Ukraine's cyber war, repelled attacks and effective strike methods are currently only known to the parties to the war. At the moment, operational information on best practices is preserved so that awareness of one's own capabilities or how much of another's actions can be detected does not flow to the enemy. If and when peace is established, it is possible that these lessons will end up in wider awareness, either in the operations of war-hardened Russian hackers on Western countries or as important lessons on how Ukraine has managed to repel attacks.



Events of Ukraine's Cyber War



Viasat satellite network KA-SAT

DATE: 24.2.2022

DESCRIPTION: The first cyberattack of the large-scale invasion of the war in Ukraine and the "starting shot" of the cyber war. Hours before the ground attack began, Russian hackers carried out a data-destroying wiper attack on the satellite service provider Viasat's KA-SAT satellite network. More specifically, the target was the system's ground station in Italy, and the aim was to disrupt the communications connections used by the Ukrainian authorities. The

perpetrator is suspected to be hacker groups under the GRU.

IMPACT: The attack paralyzed almost all modems using Viasat's connections in Europe, and a German energy company, for example, lost control of thousands of wind turbines and tens of thousands of private users suffered from internet outages. However, the impact on the communication of the Ukrainian authorities was probably significantly smaller than hoped.



Vulkan files data leak

DATE: 24.02.2022

DESCRIPTION: A data leak of a Russian company called NTC Vulkan in the first days of a large-scale attack. It is a medium-sized Russian information security company, which founders have a background in the Russian armed forces. The leak occurred from within the company, when an anti-war employee handed over thousands of internal documents to the German media, which revealed connections to Russian state-sponsored hacker groups and information about their operations.

IMPACT: Western intelligence services obtained a significant amount of information about the techniques and tactics of Russian APT groups, as well as how strikes are prepared and planned. The company was revealed to have connections to hacker groups under both the GRU security service and the SVR. The company had acted as a subcontractor and developer of tools for the above.



KyivStar

DATE: December 2023, the attack took place on 12.12. The effects continued for weeks.

DESCRIPTION: One of the most significant and publicized Russian cyber operations against Ukraine. The target was one of the country's largest telecom operators, Kyivstar, and the attack was carried out by the hacker group Sandworm, which is linked to the GRU. According to estimates, the systems had already been infiltrated months earlier before launching the attack. Attack itself was a wiper attack, i.e. the goal was only to destroy data and prevent the systems from working.

IMPACT: Thousands of telecom operators' servers and information systems were completely wiped out and about 24 million users lost mobile internet access for days. This led to users not receiving warnings from the state about air strikes or missile strikes on their territory, among other things. Kyivstar suffered financial losses worth several millions, but still did not collect the January invoices from its customers as an apology for the interruption in operations. It is not known that the attack has had a significant impact on the Ukrainian armed forces or their communications.



Attacks by Russian hacktivist groups across Europe

DATE: From the moment the large-scale invasion began to the present day.

DESCRIPTION: Several Russian hacktivist groups, such as Noname057(16) and Killnet, have carried out daily cyberattacks against European targets. The attacks have mainly been denial-of-service attacks, but there have also been website defacement and sometimes even data breaches. However, most of the attacks cause only a very small or temporary inconvenience to their victims, and their main purpose is not really to cause damage, but to get a reason to

repost on Telegram channels. Another goal that was achieved well in the early stages is to cause uncertainty and fear in the target society. Although denial-of-service attacks were sensationally reported and may have caused confusion, they were soon identified as relatively harmless, and this effect weakened.

IMPACT: Hacktivist operations have not had long-term or significant effects. They may cause momentary interruptions in the availability of the targeted websites, but in these cases it may also be a matter of the service owner restricting traffic from abroad.



Space Meteorological Research Center "Planeta"

DATE: 24.1.2024

DESCRIPTION: Ukraine's intelligence service GUR announced that it had carried out a data breach against the Russian Space Meteorological Research Center. In its report, the GUR announced that the attacker was a hacker group called BO Team, which consists of Ukrainian volunteers.

IMPACT: According to Ukrainian reports, tens of

millions of files and even physical hardware were destroyed as a result of the attack. Russian sources, on the other hand, denied the attack's success in its entirety. The research center controls dozens of satellites, so the goal may have been to influence the communication systems of the Russian armed forces or authorities, but of course this impact has also been denied by Russian sources.



REFERENCES :

Cyberwatch Finland, reviews 2022–2025

<https://kyivindependent.com/ukrainian-military-intelligence-disrupts-gazproms-digital-services/>

<https://www.ukrinform.net/>

<https://aif.ru/politics/world/zelenskiy-dovyol-trampa-kak-prohodyat-peregovory-mezhdu-ssha-i-rossiy>

<https://www.securityweek.com/kapeka-a-new-backdoor-in-sandworms-arsenal-of-aggression/>

<https://www.thesign.media/blog/cyberattack-on-viasat-satellites-eu-accuses-russia>

<https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview>

<https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat>

<https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html>

<https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics>

<https://therecord.media/ukrainian-hackers-hit-russian-scientific-center>

<https://cip.gov.ua/en/news/cyber-operations-rf-h1-2024-report>

<https://nsarchive.gwu.edu/sites/default/files/documents/rmsj3h-751x3/2022-11-28-CNMF-Before-the-Invasion-Hunt-Forward-Operations-in-Ukraine.pdf>

<https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=64622&embedded=true&a=bi>

<https://www.withsecure.com/en/whats-new/pressroom/withsecure-uncovers-kapeka-a-new-malware-with-links-to-russian-nation-state-threat-group-sandworm>



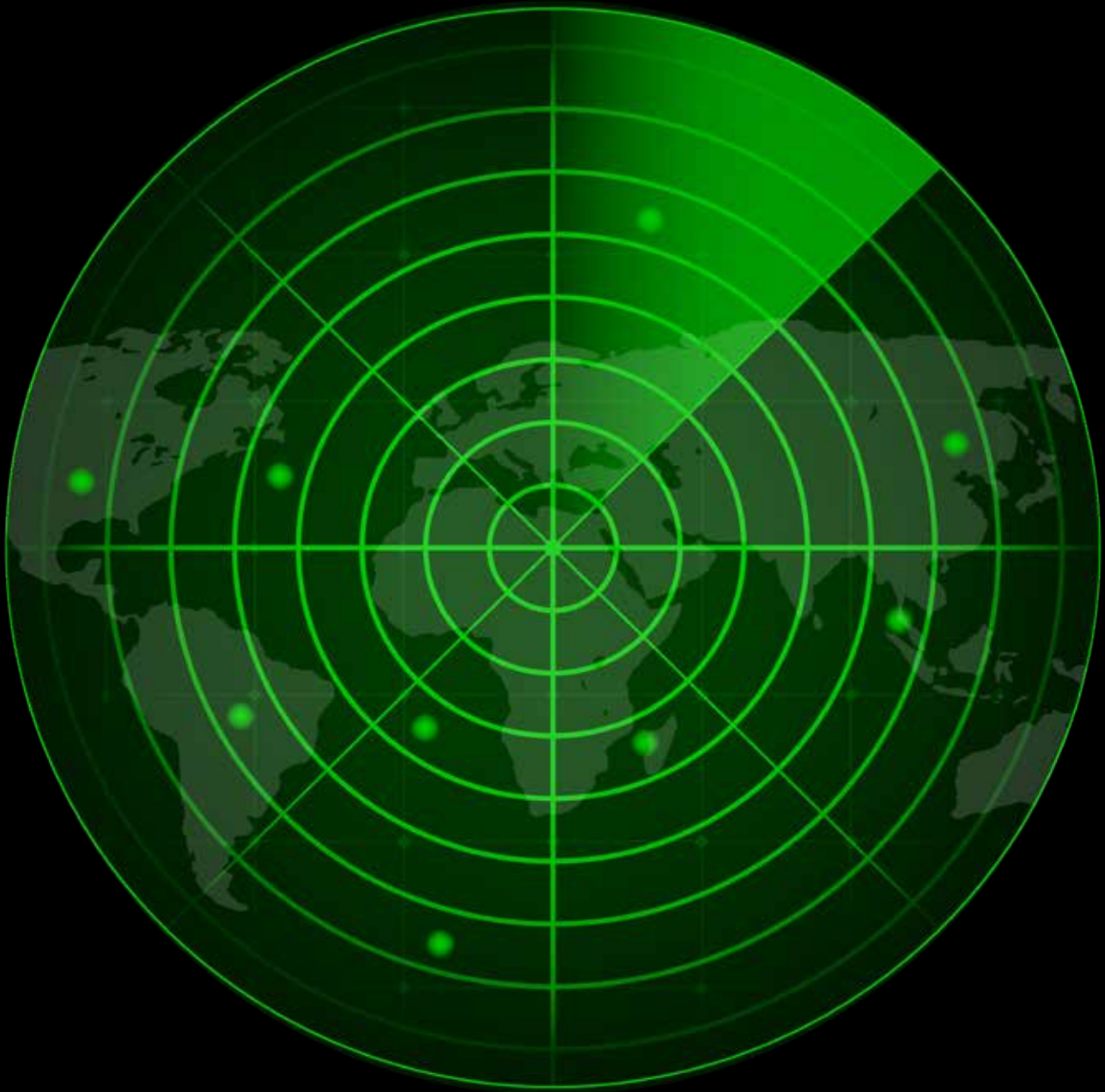
A Passion for a Safe Cyber World



Cyberwatch Finland



Cyberwatch Finland



MONTHLY REVIEW

MARCH/2025



Cybersecurity is Built by Small Actions and Management of Large Concepts

CONTENT :

EVENTS IN THE CYBERLANDSCAPE

IN THE SPOTLIGHT

- » Change in Russian APT group's targeting.
- » Excerpts from the Munich Security Conference.
- » Doge caused unnecessary cyber risks.

FOLLOW THESE

- » Are open-source projects in crisis?
- » Poland trusts Google, public-private cyber cooperation offers opportunities.

THREAT INTELLIGENCE REVIEW

- » Major cyberattacks and campaigns.
- » Active and rising threat actors.



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.

With regard to February, we highlight the changes

in the targets of Russian APT groups, the cyber aspects of the Munich Security Conference, and the lessons learned from the actions of the US Doge in terms of cyber security. The topics to be monitored include the future of open source projects and perspectives on public-private cyber cooperation, such as the cooperation between Poland and Google, which deepened further in February.




1 EVENTS IN THE CYBERLANDSCAPE

There is a well-known saying from history that sometimes more things happen in weeks than in decades. Looking at the events of February and early 2025, an analogy cannot be avoided. During February alone, a lot has happened globally: in the United States, Trump started significant changes in the country's administration, and these have also had a clear impact on the cyber environment. Regardless of what one thinks of Trump or his policies, it is undeniable that the changes caused by the rise to power will be felt globally in many different fields, and there will be plenty of material for analysis for historians and political researchers to come for a long time to come. At the same time, in February, the war in Ukraine reached its third anniversary and the event seemed to be marked by a discussion about the armistice, in which, however, Ukraine itself was not involved all the time. Negotiations were held between the United States and Russia, as well as at the Munich Security Conference. European countries have spoken loudly about the importance of continuing to support Ukraine. It would not be an understatement to say that we are currently living through significant moments that could form the basis of the European security environment for years to come.

All of this also has a direct impact on the cyber environment. International politics affects both state APT activities and cybercrime that is separate from it. For example, the activities of hacker groups linked to Russia are significantly affected by whether they want to de-escalate or escalate relations with the West. At the same time, changes in the US administration are affecting cybersecurity, and concerns have been expressed, among other things, about the extent to

which cuts in the administration's cybersecurity experts will affect the ability to counter or analyse external threats. This may lead to an increasing transfer of cyber expertise to private actors, especially international technology companies.

In the midst of major changes, it should not be forgotten that cyber security still relies on the technologies in use and their utilisation. During the month, the Chinese artificial intelligence DeepSeek, which appeared out of nowhere at the end of January, which seemed to have been able to boost the production of AI applications many times more than that of Western competitors still remained in focus. Although it is not possible to verify the accuracy of all the claims, it is still clear that we are currently living in some kind of golden age of artificial intelligence. New ground breaking applications are constantly being published at the same time as the resources required for their development are becoming cheaper and cheaper. As an example, Elon Musk's xAI startup released the new Grok-3 AI, which seemingly is decisively more efficient than current applications in terms of performance. So far, only a fraction of the potential of artificial intelligence has been exploited. For example, in February, the head of Google Labs told the online magazine Wired that even if the development of new capabilities were stopped now, there are enough untapped innovations in stock to have enough performance that can be converted into products for the next 5–10 years. The statement probably contains some exaggeration, but it gives some indication of how the power of artificial intelligence is currently growing faster than there is time to come up with applications for it.



2 IN THE SPOTLIGHT

2.1 Change in Russian APT group's targeting

In February, Microsoft published a report on a subgroup of Russian hacker group known as Sandworm, APT44 and Seashell Blizzard, among others, whose activities it had monitored and analyzed for several years. Not only have the geographical targets of the group's attacks changed during the war in Ukraine (first only Ukraine, then its allies and, in 2024, especially English-speaking Western countries), developments have also been observed in the operations themselves that can be considered exceptional for an APT group. Usually, when talking about state-sponsored APT groups, well-planned and long-prepared attacks with carefully selected targets come to mind. However, according to Microsoft's report, there has been a change in the group's operations in the selection of targets for attacks.

Microsoft's report talks about a "spray and pray" mode of operation, which describes relatively random target selection and the exploitation of commonly known vulnerabilities. The Sandworm group has been observed to scan the external network assets of organisations in a selected target country with publicly available tools (or similar solutions), and select its target simply based on where it is easy to carry out the attack. Only after the systems have been broken into it is examined what kind of organisation it actually is, and whether the attack on it or the information that can be stolen has a strategic benefit. In the occasions that the breach has been found to be useful, the operation has continued by penetrating deeper into systems and stealing valuable information. Microsoft's report does not specify which targets the group has been found to have penetrated in this way, and in which the attack has been abandoned due to minor significance. However, it is likely that the targets where the attack has continued are those that would not otherwise have risen to the lists of threat actors, but are part of the subcontracting chains of critical actors or government agencies. For example, it can be a subcontractor, a subcontractor of a subcontractor, or a company that provides IT services for some part of the chain that might not otherwise have been identified

as part of the chain or as a potential vector for critical information.

Cyber defenders must take note of the change in operating methods, as this will have a significant impact on which companies or organizations are at risk of being targeted by the APT group's operation. In the future, every organisation must take the threat into account in its operations. Subcontractors of critical organisations, who are likely to be the first targets of this type of strike campaign, are in a special position. The threat can be significantly reduced with easy measures that require very little effort. Managing one's own external infrastructure and actively updating vulnerabilities significantly reduces the risk of being attacked. The same scanning that APT groups are now doing can be done by the organisation itself and it can be used to identify gaps before they can be utilized. In addition to preventing the most common attack methods (which Sandworm had also used), it gives a potential scanner an image of an organisation that takes cybersecurity seriously and takes good care of security and is therefore unlikely to have other gaps in its systems.

Even though the attack was usually not continued in this attack campaign, if the target was found to be "worthless", non-critical actors should not be lulled into sense of security by this either. In recent years, the activities of APT groups have often been associated with a financial motive, and even if the target has no strategic value, it can still be demanded to pay a ransom, for example. Hackers from Chinese APT groups have even been suspected of carrying out ransomware attacks like this as a "side business" to targets that have been successfully penetrated but whose data has no strategic value to the state. In addition, successful intrusion does not always have to be exploited by oneself, but it can be sold, for example, in which case it is quite easy to turn it into a monetary benefit. Whether it's a critical actor, its subcontractor, or an organization that is completely detached from this chain, the likelihood of APT attacks seems to be increasing, and responding to the threat requires a response.

2.2 Excerpts from the Munich Security Conference

From 14 to 16 February, the traditional Munich International Security Conference was held. The conference consisted of high-level meetings, speeches, panels and meetings with security experts. There was also a lot of talk and discussion about cyber and technology security, although the main focus of the event was on the war in Ukraine, possible future negotiations and peace plans. The Security Conference has traditionally focused on issues at the strategic level.

The event included several speeches and panel discussions that either directly or indirectly dealt with cyber security. Artificial intelligence, in particular, was discussed in several contexts. For example, in the panel discussion "Ai Just Can't Get Enough: Disinformation, Ai, and Democracy", which directly dealt with artificial intelligence, attention was drawn to the challenges and new risks brought about by the rapid change in technology. The panel discussed the slow decision-making process in democracy and how to encourage innovation but also regulate technology and the risks it brings. The EU, in particular, has wrestled with what is necessary regulation and what restricts innovation and development too much. The U.S. perspective has been a "business-first" mentality. Companies have been allowed to innovate and create economic growth, and regulation has been dealt with later. Perhaps the EU should also reconsider its own approach more closely. The dilemma is how to allow companies to innovate enough and grow enough without interfering or placing too many demands on the technology and its use, while at the same time preventing the illegal use of new technologies.

In other panels that touched on the topic, it was stated, that artificial intelligence itself is a very anti-democratic technology. AI centralizes power in the hands of AI holders, makes it easy to engage in mass surveillance, and is also highly manipulative and hallucinating. Artificial intelligence is a perfect fit in the toolbox of authoritarian states. Large part of discussion was related to the regulation of artificial intelligence and how artificial intelligence can achieve a lot, for better or for worse. Many parties warned of Russia's growing capabilities in the use of artificial intelligence, for example in spreading disinformation and carrying out cyber-attacks. In addition, the connection between artificial intelligence and cybercrime and whether artificial intelligence will massively increase the number of attacks carried out by cybercrime were

discussed. There are already indications that artificial intelligence can be used to produce malware and carry out large-scale attacks.

The technology competition was also on display. For example, the panel "All Bits Are Off: The Risks of Racing for Tech Dominance" discussed the technology competition, the current situation, and the need to understand the situation as a competition in general. The perspectives included the confrontation between the West, China and Russia, as well as different approaches to winning the competition. Attention was drawn to the self-evident position of the West as a pioneer of technology, which has continued for several decades, and which has been changing in recent years. The panel discussed whether the winning strategy is to respond to the competition with sanctions and strict tariffs or by focusing strictly on one's own innovation and technological development.

At the conference, there were also speeches about whether the next debate will be about forcing technology to bend to a democratic environment, taking into account privacy and human rights, or about the democratic political system and the free world bending more towards autocracy with technology. As an example, the situation has already deteriorated in the sense that many companies are engaged in micro-profiling of their application users, which makes it possible to influence their thinking. Technology no longer necessarily serves the individual, but individuals serve the technology and the companies that control these technologies. The democratic world should ensure that people have a genuine opportunity to decide about their own data and the use of their own data – what data is and is not disclosed, and what is done with the collected data and what is not. In addition, artificial intelligence can also serve as a useful additional capability and, for example, in a panel discussion on future intelligence methods, it was mentioned as a possible tool that enables the intelligence services of small states to produce valuable information without large resources.

Overall, the Munich Security Conference highlighted many important issues related to cyber and technology security and brought experts and decision-makers together to discuss topical issues. One can read and listen more about the matter on the conference website: <https://securityconference.org/en/msc-2025/>



2.3 Doge caused unnecessary cyber risks

In the United States, the new agency Doge (Department of Government Efficiency), appointed by President Donald Trump, has caused widespread attention due to layoffs and other measures it has implemented. The Doge was established by decree of the President, and its legislative status and powers are, in a word, unclear. From the perspective of cyber security, the exceptional measures have caused significant and unnecessary risks. While it is not yet possible to prove that sensitive information has been leaked into the hands of threat actors, a look at Doge's recent actions provides a good reminder of the need for basic security and cybersecurity practices.

The first lesson offered by Doge is related to who is given access to critical information systems and on what grounds. Apparently, no background checks had been carried out on the Doge employees who had access to sensitive and encrypted documents and systems of US agencies, and access to the information systems has been obtained by pressuring and laying off security personnel. There has also been a case in the headlines where a Doge employee had accidentally obtained access to a code that controlled the payment of federal tax refunds, social security contributions, and more. The broad access rights granted violate the principle that access should only be granted to material for which there is a justified and genuine need. The case highlights the importance of identity and access

management in securing one's own and customers' information.

The second risk concerns the organization's cyber security training and the rules of the game and overlaps with the previous consideration of the lack of background checks. There is no information on whether the individuals have training or know-how in the basics of cyber security or data protection. Carefree practices and lack of training are clear risk factors that every organization should identify.

The third risk concerns the general confusion caused by the events. The monitoring of the actions is clearly inadequate, and the measures have been taken in a hurry. Hurry, lack of overall management and inadequate controls provide threat actors with an attractive window for misuse, such as data theft or infiltration of systems, as data breaches can go unnoticed in the midst of chaos. In ordinary organisations, this can be seen in crisis situations, changes in the organisational structure, or other situations that require a sudden response. However, changes should be avoided at the expense of safety.

Regardless of the organisation, the chaos caused by Doge provides a good lesson in the basics of cybersecurity. Identity and access management, personnel training and good overall management form the basis for building comprehensive cyber security.



3 FOLLOW THESE

3.1 Are open-source projects in crisis?

Open-source projects are key components of the internet's infrastructure and modern online services. There are a huge number of open-source projects that cover a large part of the internet's important areas. Many open-source projects serve as a basis for various operating system functionalities, and they are also borrowed a lot in application development. For example, the gap in the XZ utils project that emerged last year would have affected practically all Linux operating system devices, i.e. millions of computers and servers around the world, if it had ended up in distribution.

For a long time, various open-source projects have faced challenges and problems. Often, the projects are very small in terms of funding and resources and are based almost entirely on the unpaid work input of volunteers, which makes it difficult to develop and maintain the projects. This setup is the source of several other problems in open-source projects. The motivation and commitment of developers are often put to the test when, in addition to their own work,

they strive to maintain and develop projects that do not have funding or that do not necessarily involve other people or only a few other helping hands. Maintaining projects and, for example, being responsible for product safety with non-existent resources can be challenging. Over the past few years, there have been increasing indications that these projects have been infiltrated with content that could enable external attacks, and there is justifiable concern about the ability and resources of volunteer developers to protect the projects from these efforts. The original developers of the project may also lose interest and move on to new challenges, risking that the maintenance of the projects will cease altogether. Open-source projects are communal activities. Experts in the field, interested coders and end users of products often work together to maintain, develop, comment on and use open-source applications and projects. This also creates challenges. Various conflicts may arise within the community, which make it difficult to develop and maintain the project. An example of this came in early



February, when disagreements and outright disputes arose between the key people of the Rust for Linux (R4L) project. As a result, some of the developers ended up leaving the project.

The future threat to open-source projects is the aging developer community. The younger generation, as before, does not commit to maintaining the common good without a clear and motivating reward for work. Various resourcing solutions have been proposed for this, in which parties using the applications of the projects would start actively sponsoring these development and maintenance work, in which case the developers could be paid. According to statistics, more

than 60% of open-source developers do not currently get paid for their work, rather work is inspired by hobbies and the common good that comes alongside.

Many organisations utilise open-source projects in their IT systems, such as the Linux operating system or various web servers and relational database management systems. If the number of developers in open-source projects continues to decrease, it will create a wide range of security risks through maintenance and development problems. Organisations can also be active and offer to sponsor the projects they use and create active discussion and a positive sense of community around open-source development.

3.2 Poland trusts Google, public-private cyber cooperation offers opportunities

In February, Poland and Google signed a new memorandum on digital cooperation and investments. The background is a long-term collaboration, which has already started in 2014, when Google established its own start-up campus in the country. Over the years, the collaboration has evolved and, for example, in 2022, Google announced that it would invest 700 million dollars in Poland. The goal of the new cooperation is to invest billions of euros more. According to Google's own estimates, the investments could increase Poland's GDP by as much as eight percent. The goals mentioned involve the deployment of AI solutions in Polish companies and organizations, especially in the energy sector and cybersecurity. The memorandum also includes a section on Google's participation in the development of poles digital skills.

The cooperation is based on mutually beneficial goals and previous positive experiences. The collaboration with Google is financially significant for Poland and has historically supported the development and ecosystem formation of the IT sector, including cybersecurity. The recent memorandum promises support for cybersecurity and the energy sector, which is strategically significant as Poland is one of the most popular targets for Russian hackers. Google is also one of the most significant companies in the field of information security and artificial intelligence. Poland can benefit from this expertise and cooperation. **Poland has** invested in the availability of labour in particular, and the country has marketed itself as a

centre of digital competence and education in Eastern Europe. At the moment, there are an estimated 400,000 IT workers in Poland. The National Digital Strategy for 2025–2035 sets the goals of building a new supercomputer, building an "AI factory" and directing investments in cyber security and artificial intelligence. This has created a favourable operating environment for IT companies such as Google. For Google, the relatively lower labour costs and the operating environment that allows it to learn new lessons from, for example, Russian cyber-attacks, are also attractive.

Although cooperation between the public and private sectors is at its best fruitful for both parties, and the Finnish comprehensive security model also emphasises cooperation between companies and authorities in the sector, the cooperation is not entirely risk-free. From the point of view of national security, it may be detrimental if cyber defence starts to rely too much on foreign profit-seeking companies. On the other hand, it has long been the case that the most significant expertise in cyber security is in the private sector. It is a difficult dilemma - how to keep the cooperation balanced and sustainable in terms of national security. Cooperation with major internet companies is likely to guarantee access to the latest technology and the most modern operating methods. At the same time, it would be important to invest in one's own national performance by maintaining capabilities in the authorities and, for example, by investing in national startups and education.



REFERENCES :

Events in the cyberlandscape

Cyberwatch weekly reviews in February 2025

<https://www.bbc.com/news/articles/cm292319gr2o>

<https://www.theguardian.com/technology/2025/feb/18/elon-musk-grok-3-ai-chatbot>

https://commission.europa.eu/news/eu-reaffirms-unwavering-support-ukraine-anniversary-invasion-2025-02-24_en

Change in Russian APT group's targeting

<https://thehackernews.com/2025/02/microsoft-uncovers-sandworm-subgroups.html>

<https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/>

<https://www.darkreading.com/cyberattacks-data-breaches/chinese-apt-emperor-dragonfly-ransomware-attack>

Excerpts from the Munich Security Conference

<https://securityconference.org/en/msc-2025/>

<https://therecord.media/munich-cyber-security-and-security-conference-2025>

Doge caused unnecessary cyber risks

<https://therecord.media/treasury-fully-aware-of-risks-posed-by-doge-access-to-database> <https://www.washingtonpost.com/business/2025/02/25/elon-musk-doge-data-privacy-security/>

<https://www.hs.fi/maailma/art-2000011017558.html>

Are open-source projects in crisis?

https://www.theregister.com/2025/02/16/open_source_maintainers_state_of_open/?td=rt-3a

<https://explore.tidelift.com/2024-tidelift-survey/2024-tidelift-state-of-the-open-source-maintainer-report>

https://www.theregister.com/2025/02/13/ashai_linux_head_quits/

https://www.theregister.com/2025/02/07/linux_torvalds_rust_driver/

<https://lkml.org/lkml/2025/2/6/1292>

<https://www.linuxfoundation.org/blog/open-source-maintainers-what-they-need-and-how-to-support-them>

<https://www.techzine.eu/news/security/118829/vigilance-required-to-counter-infiltration-attempts-of-open-source-projects/>

Poland trusts Google, public-private cyber cooperation offers opportunities

<https://www.gov.pl/web/primeminister/google-invests-billions-in-polands-digital-future>

<https://blog.google/around-the-globe/google-europe/increasing-googles-investment-in-poland/>

<https://www.securityweek.com/google-hub-in-poland-to-develop-ai-use-in-energy-and-cybersecurity-sectors/>



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



SIGNAL TARGETED BY A PHISHING CAMPAIGN

DATE: Operation detected in mid-February 2025
DESCRIPTION: Hackers linked to the Russian regime have exploited the "Linked devices" feature of the Signal messaging app in phishing attacks on representatives of the Ukrainian armed forces. Infected QR code links disguised as group invitations were sent to those targeted by phishing. In addition, the Sandworm group (APT44) of the Russian military intelligence agency GRU has been found to have used the same "Linked devices" feature to take over

the Signal accounts of phones seized from the battlefield.

ACTOR: UNC5792 & UNC4221 & APT44

MOTIVE: War

IMPACT: Signal patched the issues identified in its new app update, and so far, they have been found to prevent the further use of this attack technique. The incident highlights the vulnerability of messaging applications.

DATA LEAK OF DANISH PROPERTY OWNERS

DATE: February 2025

DESCRIPTION: A database of Danish property owners was leaked online. The database contained information on 3.5 million people, including names, addresses, dates of birth and organisational information.

ACTOR: Unknown

MOTIVE: Unknown

IMPACT: The data of 3.5 million people ended up online. This information can be used in future criminal activities, such as in support of identity theft. The case is an example of how much data and how much impact can be in a data breach made in a single database.



CRYPTO BROKER BYBIT UNDER ATTACK

DATE: 21.2.2025

DESCRIPTION: Cryptocurrency broker ByBit experienced a cyberattack suspected to have been carried out by North Korean hackers. The attack targeted the company's internal migration process, which involved moving Ethereum from the offline repository to the online repository. The stolen cryptocurrencies were initially transferred to crypto wallets, which were identified as wallets previously used by the Lazarus group. The attacker had subsequently released its own crypto coins, through which the attacker laundered stolen cryptocurrencies. The attacker had also transferred some of the cryptos to various crypto mixers that

mix cryptocurrencies with other currencies using the service. In this case, it is almost impossible to track and trace them.

ACTOR: Lazarus (North-Korean APT38)

MOTIVE: Economic

IMPACT: ByBit lost about 1.5 billion USD worth of Ethereum cryptocurrency in the attack. It is not yet known whether anything will be returned to the company. The ByBit company is likely to make huge losses as a result of the attack but assures that all of its customers' funds are still safe and that it bears responsibility for what happened. The case is an example of criminal activity carried out by North Korea to finance its economy and nuclear program.

Active and rising threat actors



CLOP

DESCRIPTION: The Russian-speaking Ransomware-as-a-Service (RaaS) actor first emerged in 2019. Targets its attacks mainly on the health, financial, media, industrial and education sectors. Most targets of attacks are in Western countries, especially in the United States.

RECENT ACTIVITY: The group has been by far the most active ransomware actor in 2025. More than a thousand ransomware attacks have been carried out with the group's products during the beginning of the year, with the number increasing daily.

METHODS AND TACTICS: In its operations, Clop

makes use of targeted phishing in particular, as well as vulnerabilities in applications and various systems. Its attacks have been found to have been interrupted after the victim was found to speak Russian or another language of the former Soviet Union. Clop implements the quadruple blackmail method of their attacks. It steals and encrypts the victim's databases. It threatens the victim with DDoS attacks if the ransom is not paid, and also contacts the victim's customers and employees, threatening to publish their private information if the ransom is not paid.



LUMMA STEALER

DESCRIPTION: Malware-as-a-Service (MaaS) actor has been active on Russian-language forums since at least 2022. The malware is believed to be developed by a 'Shamel' threat actor that sells the malware on Telegram, as well as on dark web sales platforms.

RECENT ACTIVITY: Lumma publishes weekly Lumma Malware Logs, which include, for example, login information, cookies, and crypto-wallet information. Primarily, this information is sold on various platforms on the dark web, but some of it is published for free. Eventually, free information ends up on several other dark web lists, which remain cir-

culating as part of larger "Credential Stuffing" combo lists. These lists can be exploited by countless different cyber threat actors in their various criminal activities.

METHODS AND TACTICS: Recently, Lumma has been exploiting fake CAPTCHA verification pages, in particular, to trick the user into executing malicious PowerShell commands. Various pirated applications have also been found to contain the Lumma malware. These applications have been advertised on Telegram and YouTube videos, among other places.



STORM-2139

DESCRIPTION: In February, Microsoft identified and named members of the international cybercrime group Storm-2139. Citizens of Iran, the United Kingdom, China and Vietnam, among others, were found to be involved in the activities of the criminal group.

RECENT ACTIVITY: Storm-2139 has actively sought to break the rules of various service providers' AI applications by creating its own technical tools that have been used to circumvent the rules. The aim has been to misuse and use artificial intelligence in cybercrime, including deepfakes. The group's activ-

ities demonstrate the suitability of new technologies for cybercrime and its international and cross-border nature.

METHODS AND TACTICS: Storm-2139 is divided into three levels: Developers, Providers, and Users. Developers are developing tools that can be used to misuse various AI applications. The providers modify the developers' tools into tools suitable for specific AI applications, which users then exploit for illegal cybercriminal activities. Often, the end products are, for example, sexual material of public figures.





Our mission:

MAKE CYBERSECURITY A BUSINESS OPPORTUNITY

Cyberwatch Finland serves companies and other organisations by strengthening and developing their cybersecurity culture.

Increasing regulation improves cybersecurity in all organisations, but compliance with the minimum requirements is not enough in the ever-tightening competition. A high-class cybersecurity culture is a competitive advantage and creates new business opportunities.

Our strength is a unique combination of profound know-how and extensive experience

Our team of experts consists of versatile competence in strategic cybersecurity, complemented by extensive experience in management, comprehensive security and operations in an international business environment.

Our experts know how to interpret and present complex phenomena and trends in the cyber world in an easy-to-understand format. Our work is supported by advanced technology platforms as well as modern analysis tools.

We help our clients stay up-to-date and consistently develop a cybersecurity culture. At the same time, we are building a more sustainable and safer world together.

Aapo Cederberg, CEO and founder, Cyberwatch Finland

Cyberwatch Finland is a strategic cybersecurity consultancy house that provides professional services for companies and other organisations by strengthening and developing their capabilities to protect and defend their most significant assets.



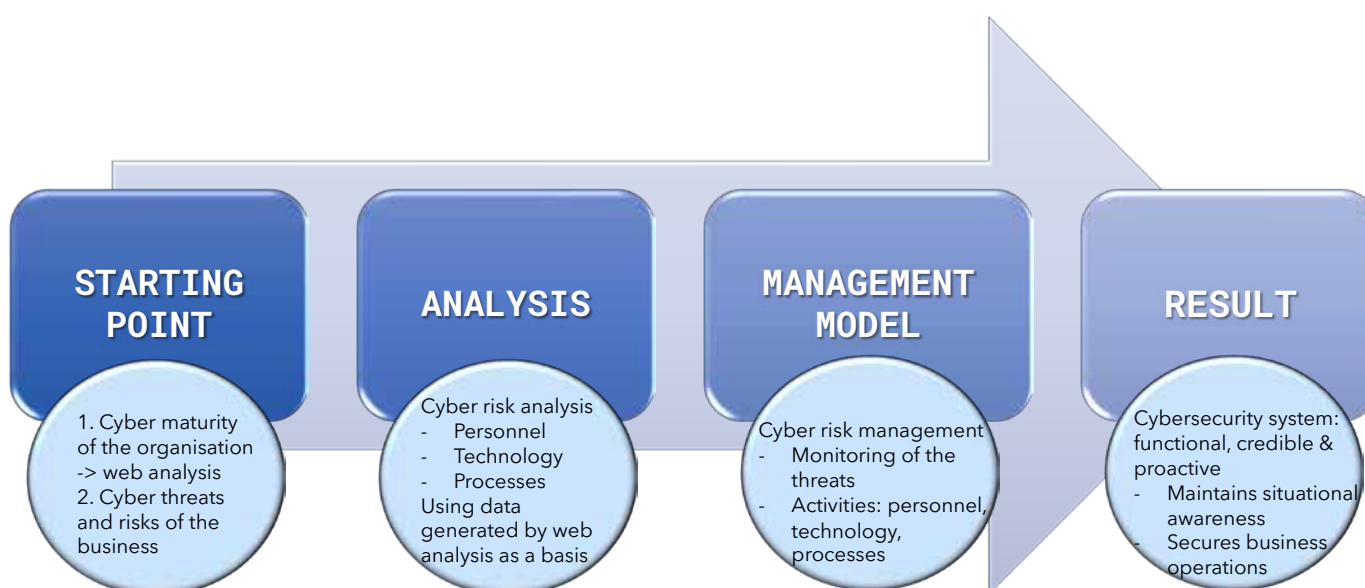
Cyber risk management model

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 how to implement the required actions the increasing EU regulation and national legislation has brought.

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



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 includes 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)

Operational environment analysis

Cyberwatch's analysis team constantly monitors the cybersecurity operational environment by collecting and analysing information about events, phenomena and

changes in the cyber world. The situational picture is produced by regular situational reviews.



WEEKLY REVIEW

Weekly reviews introduce the current events of the cyber world. The focus of the weekly review is 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 the 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 about 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 the most significant cyber events, phenomena, trends and their interdependencies of the previous month, 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 forecasts.

Web analysis - darkSOC®

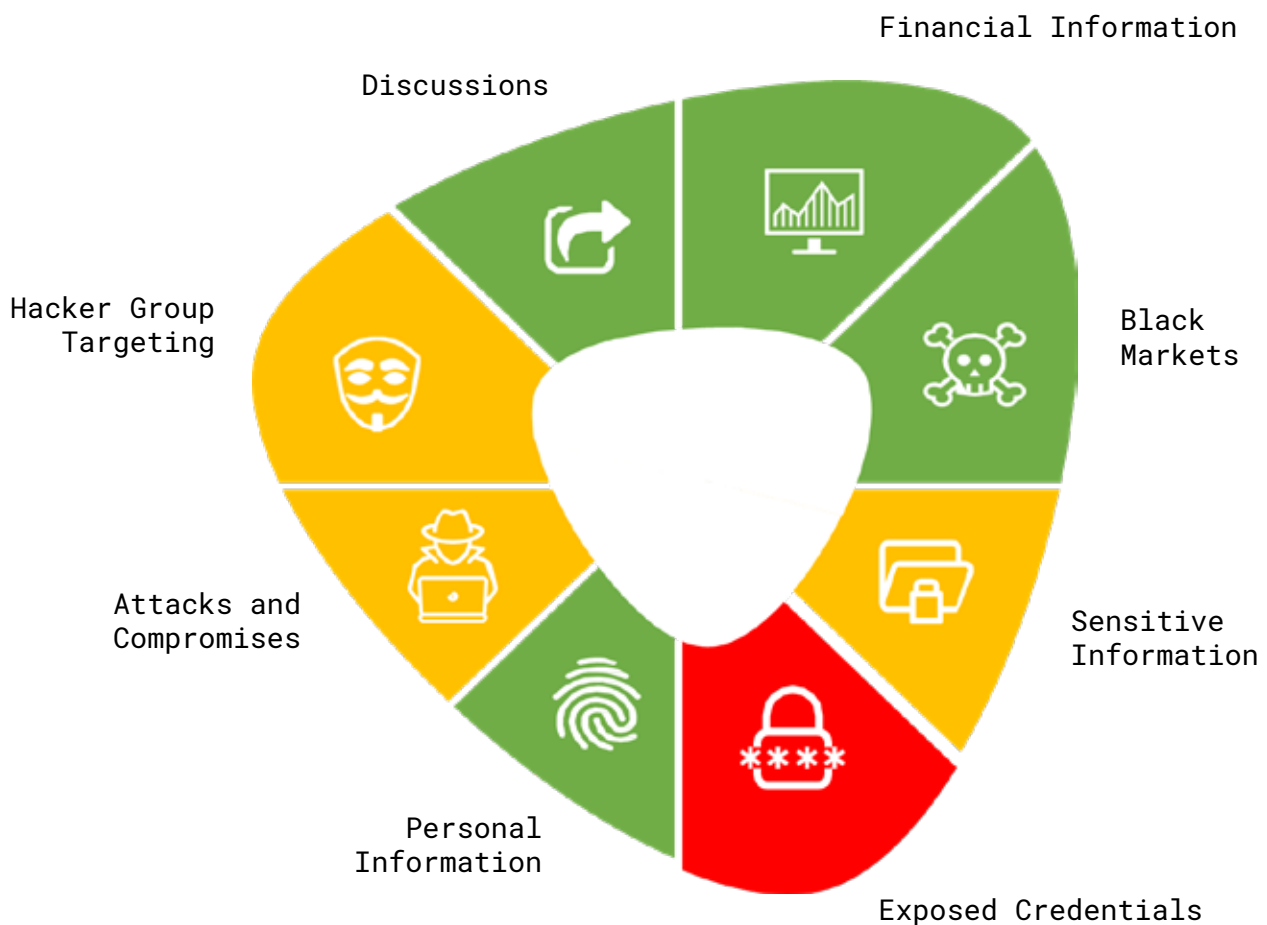
WEB ANALYSIS

In our web analysis, we examine and report your organisation's profile and level of exposure in the dark and deep web. The analysis reveals organisation's cybersecurity deficiencies, data breaches, and other potential vulnerabilities. Web analysis contains attack surface analysis which analyses the structure of the organisation's network infrastructure and the state of its network's cybersecurity.

The tools used are the Cyber Intelligence House's database and Badrap's services. Data is collected non-stop at 9 Gb per second, from servers located all around the world. With the help of analysis, you get an overview of

what the organisation looks like the cybercriminal's perspective.

The exposures are classified into eight categories and based on the severity; the findings are divided into three levels. From the attack surface, it is reported how the organisation's network and the level of cybersecurity looks in the eyes of an external observer. We highlight the key findings in the executive summary to support management's decision-making. The report also includes a more detailed presentation of the findings and recommendations for the immediate corrective actions and strategic-level development targets.



MONITORING

Based on the web 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 is analysed. The results are reported at agreed intervals.

Regular monitoring:

a report delivered at agreed intervals, for example monthly, quarterly, half-yearly or annually.

Continuous monitoring:

24/7 monitoring of new findings, information about which are directly reported to the customer.

WEB ANALYSIS FOR SUPPLY CHAIN

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. 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 enables the customer, for example, in a corporate acquisition situation, to determine the cyber maturity of potential partners and to conduct a risk assessment.

Powered by:

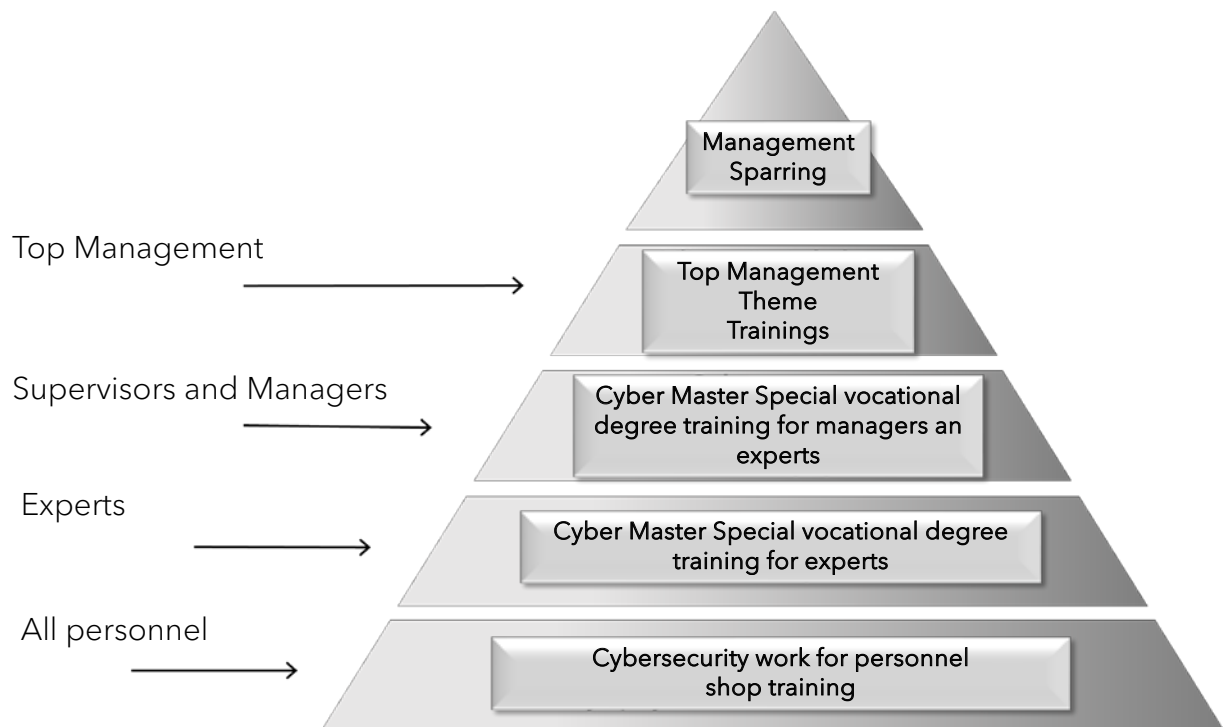


Training and competency development

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 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.



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 offering 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 face-to-face training, hybrid training or as online courses. In addition to training and lectures, you can also order scenario work for your organisation, which will help you collect and structure information that will help you understand the future as comprehensively as possible.

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.

OUR REVIEWS 2025



Contact

Cyberwatch Oy | Nuijamiestentie 5 C | 00400 Helsinki, Finland
aapo@cyberwatchfinland.fi | info@cyberwatchfinland.fi

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**

**Registration
opens
May 21st!**



4–5 November 2025
Helsinki Expo and Convention Centre

cybersecuritynordic.com