



Special media of strategic cyber security

Cyberwatch Finland

MAGAZINE 1 / 2024

HYBRID WARFARE IS ACTIVE AND CONTINUOUS INFORMATION INFLUENCING

CRISIS
COMMUNICATION
STRENGTHENS
RESILIENCE

COUNTERING
DISINFORMATION
AND FOREIGN
INTERFERENCE
AT THE TIME OF
ARTIFICIAL
INTELLIGENCE



Cybersecurity is built by small actions and management of large concepts

CONTENT

1/2024

4



HYBRID WARFARE IS ACTIVE AND CONTINUOUS INFORMATION INFLUENCING

We live in an unstable world. The war in Ukraine, the conflict in Gaza, terrorist attacks on merchant ships and regional crises in Africa are reported through all channels as a constant flood of information.

6



COUNTERING DISINFORMATION AND FOREIGN INTERFERENCE AT THE TIME OF ARTIFICIAL INTELLIGENCE

As we have witnessed during the past few years, advances in generative AI represent a massive leap forward, where AI has moved from behind-the-scenes tasks like content ranking and recommendation engines to near autonomous content creation of text, audio, video and imagery.

10



THE RUSSIA-UKRAINE CONFLICT FROM A HYBRID WARFARE PERSPECTIVE – A YEAR IN THE WAR

Russia's hybrid threat campaign against Ukraine and its surroundings prior to 24 February 2023 was a strategic masterpiece of thoughts. Neither the US, NATO nor the EU were sure what was really happening and the hybrid threat activities instilled fear in the Baltic states, Sweden, and Finland.

16



CRISIS COMMUNICATION STRENGTHENS RESILIENCE

Crisis communication aims to mitigate the impact of a crisis on the people involved. The aim is to communicate crisis scenarios and what is being done to rectify the situation from a situational picture.

18



ECONOMICAL IMPACTS OF DATA BREACHES

Companies are increasingly using digital technologies in all facets, ranging from internal operations to customer engagement. Digitalization has brought with it significant improvements to processes, efficiency, and innovation, enabling companies to create more added value for their customers.

20



COULD ALL-OUT WAR FLAME OUT IN THE BALTIC SEA REGION?

Russia's geopolitical ambitions in the European High North are on the rise. Leaked documents from the German defense ministry have revealed a terrifyingly plausible scenario for a full-scale Russian attack on the Baltic states and Poland.

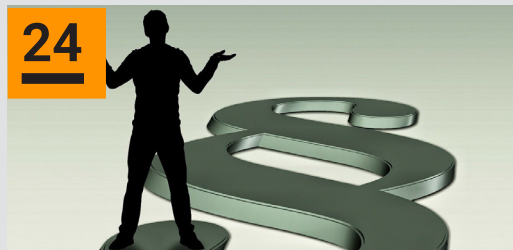
22



CYBER SECURITY NORDIC WILL BE HELD AT THE END OF OCTOBER THIS YEAR

The two-day Cyber Security Nordic (CSN) will be held this year at 29-30.10. in Helsinki Exhibition and Convention Centre

24



FINNISH INFORMATION SECURITY CLUSTERS' APPLICATION GUIDE SUPPORTS COMPANIES IN COMPLYING WITH THE NIS2 DIRECTIVE

26



SAMPLES FROM CYBERWATCH FINLAND WEEKLY REVIEWS

32



CYBERWATCH FINLAND MONTHLY REVIEW JANUARY 2024

Cyberwatch Magazine

Special media of strategic cyber security

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

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

Subeditor
Elina Turunen
elina@cyberwatchfinland.fi

LAYOUT
Elina Turunen
elina@cyberwatchfinland.fi

ILLUSTRATIONS
Gencraft
Pixabay
Shutterstock

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

PRINT HOUSE
Scanseri Oy, Finland

HYBRID WARFARE IS ACTIVE AND CONTINUOUS INFORMATION INFLUENCING

// Aapo Cederberg



We live in an unstable world. The war in Ukraine, the conflict in Gaza, terrorist attacks on merchant ships and regional crises in Africa are reported through all channels as a constant flood of information. Thus, we are constantly subject to information influence, whether we like it or not, and our sense of security can be weakened. Cyberattacks are often difficult to understand and their objectives, perpetrators or methods of implementation are usually uncertain. The knock-on effects of attacks are most clearly visible, for example, in disruptions to vital functions of society. Uncertainty causes fear and anxiety among people, as well as dissatisfaction with the reliability of services in modern society. These are often channelled as criticism towards political decision-makers and companies providing critical services. The effects can be very long-lasting and insidious.

Information warfare and influencing are often perceived as spreading false information, fake news, manipulating information and data. They are, of course, also about this. In such cases, the goal is often short-term and influencing aimed, for example, to a particular political process. Stories or narratives often seem very utopian and implausible, but their purpose may be to influence a target group or, for example, the domestic politics of an authoritarian state. Artificial intelligence is constantly creating new opportunities for data manipulation, deepfakes and various scams. Western media and citizens have learned to protect themselves relatively well from disinformation and misinformation. Less attention has been paid to analysing the information effects of various hybrid operations and protecting against them. Information effects are long-term and hide in vagueness, such as the so-called fog of war.

Russia is arguing that the battle between western civilization and the war in Ukraine is only one part of it. According to the definition of the Russian General Staff Academy, war is divided into conventional warfare and hybrid warfare. Both include physical means, i.e. military force, and asymmetric means, such as cyberattacks, information operations, political pressure, sabotage, refugee flows, economic sanctions and energy weapons. In Finland, it has been clearly noticed that we are the target of continuous hybrid warfare, aiming to create uncertainty, fear and discord among citizens and thus indirectly influence political decision-making. This form of warfare also emphasises surprise-effect, having the active initiative and various means of deception. All of these enhance the desired information effects, the success

of which requires the exploitation of the human mind and basic needs and vulnerabilities. The effects can be long-lasting and unpredictable. The "strategic weapon" of hybrid warfare is long-term information influencing, against which we must improve our protection. The target is the whole society and the mental resilience of its citizens.

NATO is investing heavily in cognitive warfare and defence concepts. The first thing that comes to mind is whether we are trying to reinvent the wheel, or whether this is really a new form of warfare? According to NATO, it is developing new forms of warfare in order to wage a "battle of the brains", as the military alliance puts it. This concept experiments with new forms of hybrid warfare against identified enemies, utilising methods such as economic warfare, cyber war, information warfare and psychological warfare. The new method is the "weaponization of brain sciences" and involves "hacking a person" by exploiting "weaknesses in the human brain" to produce more sophisticated "social manipulation." The aim seems to be not only to protect ourselves, but also to develop and utilise active means.

NATO is therefore on the cutting edge and the need to develop "hybrid defence" has been identified. As a new and active member of the alliance, Finland is also involved in this process. A good foundation is provided by the Finnish comprehensive security model and, above all, by our expertise in developing mental crisis resilience. These elements will hopefully create sufficient resilience against Russia's long-term information operations in the coming years. ■



AAPO CEDERBERG

' Managing Director and
Founder
' **Cyberwatch Finland**



COUNTERING DISINFORMATION AND FOREIGN INTERFERENCE AT THE TIME OF ARTIFICIAL INTELLIGENCE

// Pasi Eronen

As we have witnessed during the past few years, advances in generative AI represent a massive leap forward, where AI has moved from behind-the-scenes tasks like content ranking and recommendation engines to near autonomous content creation of text, audio, video and imagery.

Diffusion of these increasingly more powerful AI tools into our workflows and systems is inevitable, as innovation centers like Silicon Valley keep pushing the boundaries of what is possible.

Open AI's Chat GPT, DALL-E, and the upcoming Sora are the most obvious tools available for the general public, but there are a great number of both proprietary and open source tools available in this realm. Some of the tools come with less protective guardrails and limits for the unethical uses.

The fast-paced nature of AI development makes it challenging for researchers, policymakers,

and societies at large to keep up with the latest advances and effectively implement countermeasures against AI-generated manipulations and disinformation. This lag may leave us vulnerable to the disruptive potential of AI-generated disinformation.

Adversarial actors worldwide, such as Russia and China, and criminals alike, are taking note of the developments as well. They are acquiring, researching, developing, and deploying advanced AI-based technologies to experiment with in their information manipulation and disinformation campaigns.

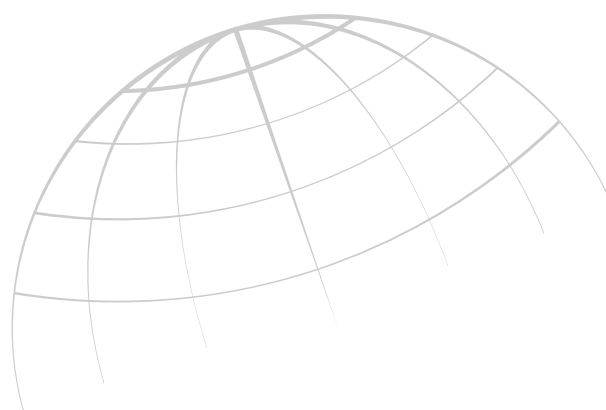
WHY SHOULD WE CARE?

The consequences of weaponized AI-enabled information manipulation and disinformation campaigns can profoundly destabilize our societies and the shared sense of security in a number of ways:

- Vulnerable and marginalized populations, such as immigrants and people struggling with participating in society and its activities, with less access to reliable information sources can be considered to be prime targets. Their trust in authorities and institutions could be systematically eroded.



AI has moved from behind-the-scenes tasks like content ranking and recommendation engines to near autonomous content creation of text, audio, video and imagery.



- Democracies could find their political processes and governance undermined by orchestrated manipulation of public opinion. This becomes an even greater issue as with technological advancements truth, or reality, becomes more indistinguishable from AI-fabricated falsehoods.
- Highly realistic deep fake media, such as fabricated photos and video, or replicated voice profiles, can psychologically devastate both prominent individuals, such as politicians or performing artists, and groups. Their reputations, and sense of privacy, can be disrupted by AI-generated fabrications.
- Social media echo chambers and filter bubbles optimized by algorithms dramatically amplify the potential impacts of disinformation, as carefully tailored content and fabrications help to establish entrenched polarized communities that are unable to agree even on basic facts and truth.
- Automated and autonomous disinformation campaigns by AI bots operating at massive scale, with minimal human oversight, will be challenging to identify and counter. Especially, if AI tools are applied in a way that allows messaging to vary according to the context, instead of repeating cookie-cutter messages across farmed fake accounts. This will also enable adversaries to quickly create and disseminate a number of “counternarratives” that can be used to muddy the waters and confuse the audiences, especially during a quickly developing situation.
- Lastly, with enough contextual understanding and AI-agent fine tuning as per targeted audiences, AI-generated content could be specifically designed to exploit existing human cognitive biases and emotional triggers. This may profoundly manipulate individual behaviors and perceptions in real world environments.





ARE THERE ANY SOLUTIONS TO THIS ISSUE?

It is fair to say that there are no simple 'silver bullet' solutions to counter the AI-enabled information manipulation and disinformation campaigns. Nevertheless, there are ways to mitigate the problem at hand.

These mitigating solutions require global cooperation, public education, media literacy, ethics and transparency in AI development, accountability for tech platforms, and continuous research and adaptation as new threats emerge:

- **Public awareness:** Raising public awareness of the potential for AI-generated disinformation is crucial in mitigating its impact. Educating the public about how to identify AI-generated content and encouraging healthy skepticism towards unverified information can help counter the spread of disinformation.
- **Education and Media Literacy:** Widespread public education campaigns and integration of media literacy into school curricula can develop citizens' and key groups like journalists and teachers skills in identifying AI-created disinformation and critically evaluating sources. This grassroots approach builds societal resilience, but is a very long-term approach.
- **Ethical Accountability:** Technologies like generative AI have significant potential for harm as well as good. Scientists and engineers developing these systems should adhere to ethical principles and be held accountable for harmful consequences. Oversight frameworks can align innovation incentives with social responsibility. Nevertheless, there is little evidence that we can compel our adversaries to follow the same ethical code as we do.
- **Global Cooperation:** Information manipulation and disinformation transcends national borders. International norms, data sharing initiatives among trusted partners, and joint funding for countermeasure development can enable a unified front against AI-amplified foreign influence. Coordinated diplomatic, economic and legal actions against state sponsors of disinformation and their operators can also act as deterrents.
- **Stronger Regulation of Tech Platforms:** Social media and content sites must be compelled through legislation to take a more active stance in moderating the content, disabling disinformation bots, minimizing algorithmic amplification of falsehoods, and being transparent about their practices, including the algorithms. Nevertheless, regulation must take into account the imbalance in global competition, where platforms developed in more legally permissive environments may get an unfair competitive edge over more regulated platforms.

- **Continuous R&D:** An inevitable "AI arms race" against adversaries requires sustained investment in detection technologies to flag AI-created media, identification of disinformation networks, and other countermeasures. Closely monitoring the evolving AI landscape is also crucial, particularly the developments in this area taking place in the adversarial countries.
- **Resilient Information Ecosystems:** Beyond reactive countermeasures, proactive efforts to build media ecosystems with trusted information curators, diverse perspectives and transparency over algorithms can make societies more resistant to manipulation.
- **Embracing Change:** Instead of reactive resistance or blind banning of AI technologies vulnerable to abuse, proactively embracing and integrating them across sectors can build deeper understanding and fuel innovation of safeguards and potential countermeasures. For example, collaboratively experimenting with generative AI in classrooms, companies and government agencies can develop best practices, reveal risks requiring solutions, and create a cohort of citizens more resilient to disinformation due to first-hand experience. A flexible, forward-looking mindset recognizes potential benefits alongside dangers.



The writing process of this article was supported by the ChatGPT-4 service from OpenAI and Anthropic's Claude service.

The path forward must balance nurturing AI's immense potential to improve our lives and workplaces with pragmatic recognition of its risks. With careful application of the mitigating solutions presented above, our societies can harness the powers of AI, while being able to maintain an open information space resistant to manipulation.

But the dangers posed by unconstrained development of generative AI cannot be ignored as our adversaries seek to unleash its dark side. We cannot stop or reverse the developments, as our adversaries are speeding forward. Thus, we have to make sure that we stay abreast, and preferably ahead of them in order to protect our societies from those that want ill for us. ■



 **PASI ERONEN WATT**

Pasi Eronen Watt is an analyst and writer focused on international security matters, specialized in information and influence operations, and cybersecurity. He has extensive experience working in the Finnish government, including international assignments.

MISINFORMATION, DISINFORMATION, AND FIMI - TELL ME MORE?

Misinformation refers to false or inaccurate information spread unintentionally due to sheer ignorance or honest mistakes. **Disinformation**, then again, is false information spread with the intent to deceive or cause harm.

Foreign information manipulation and interference (FIMI), a concept adopted both by the EU and NATO, encompasses coordinated disinformation campaigns conducted by adversarial state or non-state actors to destabilize societies, undermine trust in institutions, and interfere in political processes.

What makes a concept like FIMI particularly important is that manipulation does not need to be based on a lie, it can also take the form of artificial amplification of such organic political or other expressed views that serve the foreign adversary's agenda and political goals.



THE RUSSIA-UKRAINE CONFLICT FROM A HYBRID WARFARE PERSPECTIVE – A YEAR IN THE WAR

// Josef Schroefl and Soenke Marahrens

* This paper is based on internal and external publications of the authors at HybridCoE

THE HYBRIDITY OF RUSSIA'S ATTACK ON UKRAINE

Western military strategists have coined the acronym VUCA to describe the characteristics of the resulting future operational environment – namely, volatility, uncertainty, complexity and ambiguity or, more pessimistically, BANI, which stands for brittle, anxious, nonlinear, and incomprehensible. It can be said that the Russians have been highly dynamic in creating, either intentionally or unintentionally, VUCA or BANI conditions for the West with almost perfect precision.

Therefore hybrid war is a phenomenon still in the making. Hybrid warfare (based on hybrid threats carried out with military means in particular) is also still an interim term for the phenomenon. In a Hegelian sense, “hybrid war” can be seen as the antithesis of war in a world which situated war in international humanitarian law and finally prohibited it by making all nations sign the UN Charter. But the synthesis is still missing. According to Hybrid CoE, four characteristics of a hybrid threat activity (encapsulating threats and warfare) can be distinguished:

1. It is not a single event.
2. It needs a malign intent / actor.
3. It is conducted by authoritarian systems challenging democratic rule-based systems.
4. The Greyzone is created by the defender not the attacker, the latter is just exploiting the unwillingness of the defender to protect his/her redlines.

The antagonist exploits either the unwillingness of the rule owner to defend the rules, or the complexity of created laws and rules, which provides the malign actor with the opportunity either to misuse those rules, or to create dilemmas through the application of those rules.

RUSSIA'S WAR IN UKRAINE THROUGH A HYBRID WAR LENS:

Russia's hybrid threat campaign against Ukraine and its surroundings prior to 24 February 2023 was a strategic masterpiece of thoughts. Neither the US, NATO nor the EU were sure what was really happening and the hybrid threat activities instilled fear (or pragmatism about their own survival) in the Baltic states, Sweden, and Finland. The hybrid threat campaign was highly agile, constantly scanning for weak points in the West and addressing them almost immediately with legal, information, disinformation and diplomatic means accompanied by a rather lengthy military show of force around Ukraine, adding to the overall uncertainty. The less successful unfolding of military events after 24 February 2022, whereby the Russian forces were not able to exploit their

assumed tactical agility, may well have been accompanied by something of a strategic meltdown within Putin's inner circle. The moment that President Vladimir Putin started to publicly humiliate some of his senior leaders – the head of his intelligence service, Sergey Naryshkin, and later his Chief of Defence, General Valery Gerasimov – the necessary organizational trust may have been broken, and the organization reset into a less proactive “just follow orders” mode in order to avoid further humiliation, which not only reduced the military efficiency, but also the effectiveness of ongoing hybrid threat activities against the West.

LACK OF ELECTRONIC WARFARE: PROBLEMS DUE TO RUSSIA'S OWN COMMUNICATIONS?

After an intensive use of electronic warfare capabilities (e.g. jamming of frequencies or disturbing electronic devices like GPS equipment) during the last eight years by the Russian military in the Donbas / Luhansk region, the Western definition of the military cyber domain was recently expanded to incorporate electronic warfare as well. Hence, Western military experts assumed that Russian military operations in Ukraine would be accompanied by the heavy electronic warfare activities that had already been demonstrated in Donbas and Luhansk. But this didn't happen, different explanations are circulating among Western experts for the absence or lack of electronic warfare activities.

It looks as if Russia has been struggling with the problem of the tradeoff between jamming frequencies and the necessity to maintain command and control of its own troops by using those frequencies, as well as with the so-called “last mile” problem of how to support mobile forward-deployed forces with digital data. It appeared that the Russian forces have bypassed the problem by using Ukrainian communication networks.

Ukrainian intelligence sources published a lot of Russian military communications intercepted via internet connections through Ukrainian networks, which of course prevents Russian commanders from giving orders to shut down those networks by means of electronic warfare.

Cyber: potential equal to conventional military power. Other parts of the cyber domain add a whole new dimension to this conflict. Next to hackers, we see an unprecedented quantity of open-source intelligence through mobile phone videos, as well as a permanent game of memes and narratives in all social media outlets. Cyber,

References
on page
15



including IT and the information domain, has become as hard a power as military power. Whereas Ukraine is winning the war of memes and narratives against Russia, especially on the Western and international front, it is still hard to evaluate from the outside the extent to which the Russian population, influenced as it is by fake narratives about “denazification” and “preventing a genocide”, can be reached or influenced by the Ukrainian counter-narratives. Furthermore, we can observe a kind of applied “hybrid” thinking in the clandestine use of Russian military forces against targets in Belarus, and presumably in Luhansk, to foster Belarusian and separatist support. It is too early to evaluate the impact of the IT hacking activities. After Ukraine amassed an “army of 30,000” hackers, and after Anonymous took Ukraine’s side, it is not entirely clear what is going on in the networks. There is intense activity in the cyber domain, but it is difficult to assess whether Ukraine has consolidated its IT security sufficiently due to being permanently under attack, whether Russian troops still need access to the internet as a primary means of communications, or whether Russian troll factories are being neutralized by Anonymous.

Today, Russia’s attack, called by Russia a “special military operation” only, on Ukraine on February 24, 2022, has to be understood as a hybrid war that went rogue, but Russia’s activities after the initial failure in late February 2022 must be also analyzed and addressed as part of conventional war theory rather than part of a “hybrid war” theory only.

The operations of the Russian Armed Forces and especially their warfighting tactics have often not even met the most basic international standards set by the Humanitarian Laws of Armed Conflict, which adds an organizational or systemic dimension to the file of the observed war crimes by individual soldiers.

FROM HYBRID WAR TO CONVENTIONAL WAR

When the initial hybrid-threat approach of using land forces to coerce the Ukrainian government had failed within the first ten days, the Russian Armed Forces regrouped, even by (mis-)using safe Belarussian territory. To the utmost surprise of Western observers, they started to assume an attacking style of World War II-like mass artillery fighting rather than in a 21st-century Western-based modern warfare style based on precision-guided ammunition to reduce civil casualties. This has made the Russian operations rather atrocious and created next to civilian victims also heavy military casualties beneath the Ukrainian Armed Forces.

Next to the brutal and excessive use of military force under the statute of a military strategy called by experts “Terror,” the Center of Excellence Countering Hybrid Warfare Community of Interest for Strategy and Defense

also observed open applications of military methods in Ukraine attributed to the arsenal of hybrid warfare in sub-threshold environments: targeting and attacking systemic vulnerabilities to influencing decision-making or undermining and terrorizing the Ukrainian society.

Next to targeting military targets, Russian Forces and their proxies have started to target UKR societal system-relevant targets inside Ukraine. They conducted deliberate and repeated attacks on important railway infrastructures and power grid nodes. These attacks fit the hybrid definition as well as the definition called cross-domain effects in the Western Multi-Domain Operations terminology. In conclusion, Russia has applied an overall system-thinking approach to its warfare capabilities, allowing for more complex military operations.

Whereas the Ukrainians were able to show a very resilient railway system,^[2] the UKR power system, assumingly due to the size and need of essential infrastructures and critical spare parts, has regularly suffered heavily from missile strikes with longer-lasting power outages.

Russian disinformation experts have tried to influence the Ukrainian population through “targeted messaging” over the years. However, their efforts fell flat in light of the war crimes committed by Russian troops, e.g., in Butcha. Nevertheless, Russian propaganda addressing the “evil Ukrainians”, has been continuously successful among the Russian population. Internet polls still show a total lack of Russian empathy or sympathy for Ukrainians.^[4]

Although many Western observers were surprised by how Russia conducts its military operations, all these examples are deeply linked and rooted in their theoretical military and strategic thinking. However, for the first time, the Russian idea of reflexive control theory is similarly and parallel applied in sub-threshold hybrid warfare environments and real war environments simultaneously; whether by accident or purpose, will be seen after the war.

REFLEXIVE CONTROL

“Reflexive control is an activity which influences the adversary’s decision-making processes with a specifically altered piece of information in a prepared information campaign. The primary goal of such doctored information is to induce the other side to make decisions that are, in fact, predetermined by the producer of the doctored information.”^[6]



The concept of reflexive control has a long history in Russian military strategy. Taught in military schools and academies, it is also codified in the Russian National Security Strategy. Its elements include:

- Power pressure (provocation and deterrence);
- Measures to present false information about the situation (deception, distraction and paralysis);
- Influencing the enemy's decision-making algorithm (exhaustion, divisions and suggestion); and
- Altering the decision-making time (pacification and overload).^[7]

The foundations of Russian Reflexive control reach back more than 200 years. It follows the ideas of General Peter Rumyantsev (thought) and Alexander Suvorov (science of victory).^[8] Overall, reflexive control loosely follows the concept of one Chinese General Sun Tzu's commandments of war: "The supreme art of war is to subdue the enemy without fighting". It was updated in the late 20th century by Evgeny Messner with his ideas on subversion war – an activity that is intended to erode an adversary's socio-cultural and military cohesion – , Alexander Dugin's network-centric war – rather in a virtual dimension, establishing control over networks, more political than military, not to be mixed up with western ideas of Network Centric Warfare – , as well as Igor Panarin's Information warfare, coping with psychological and specifically informational aspects. All information means are used to target decision-making processes by manipulating international and domestic public opinion.^[9]

THE USE OF MODERN TECHNOLOGIES WITH HYBRID CHARACTER

From the beginning of humankind, war has been a relentless innovator, and Russia's war against Ukraine makes no exemption to this rule.

Cyber

Ukrainian IT systems are under permanent Russian attacks. Cyber-attacks will not cease during a conventional war. On the other hand, so-called spill-over or domino effects of offensive cyber operations – as forecasted by Western experts as an argument against the use of offensive military cyber operations – are, so far, not being observed. Finally, critical infrastructures must be identified early, protected, and defended in the physical and cyber domains simultaneously.

HYBRID THREATS AND WARFARE AROUND UKRAINE

Heavy Russian hybrid activities accompany the war in Ukraine. Russia applies almost all of the above means and methods in other operations around the world:

- Russian Private Military Companies (PMCs) acted in Africa as brutally as in Ukraine, but almost without any international reaction. The killing of 300 Malian civilians by Wagner mercenaries and Mali Army units created almost no international reaction;^[10]
- Permanent Russian disinformation campaigns through pre-established networks all over Europe and the Americas;
- The use of so-called "useful idiots" and influencers in almost all Western societies;
- Unattributed or denied attacks on pipelines and critical infrastructures all over Europe; and
- Cyber attacks on Western political leaders, especially those who have committed themselves publicly against Russia.

FIGHTING VALUE = CAPABILITIES X MOTIVATION²

Western experts or putins mainly talk about technology as the driving force behind military might or power. However, military leaders are already taught at a very early stage of their careers that the fighting value of their troops must be seen as a function of their capability (technical means / weapons) to conduct a mission multiplied by their motivation squared.

Normally that is only seen at the individual force level, but Russia's war in Ukraine demonstrates that this must be considered at a force-wide level as well. It would explain why the Ukrainian army, and their "army of volunteers", can successfully take on the mighty battle-tested Russian army.

A poor mental preparation by the Russian ground forces, leading to deserters and abandoned equipment, can also be interpreted as a sign that the Russian military leadership in particular might have seen waging war as only one possible option within the overall hybrid threat campaign against Ukraine, and hence they failed to plan adequately.

The Russians masked their initial main attack thrust axes into Ukraine – Kyiv from the North, Donbas/ Luhansk from the East and Mariupol from the South through deploying Bataillon task groups without any logistical or communication support, creating problems for Western intelligence services attempting to assess Russian intentions. Fortunately for Ukraine, the deployment did not go as planned, Russian forces have suffered from this communications and logistical setup in particular. The low morale of the troops should also be factored in, as reports from Belarus before the attack indicated that Russian units had cleared forestland for firewood and bought food with their own money.

References
on page
15





WHAT WILL RUSSIAN WAR AND WARFARE PROVIDE FOR HYBRID WARFARE AND HYBRID THREATS

The Russian military forces, Secret Services and PMCs are willing to apply inhumane brutality and violence even in light of the public. Western assumptions that covert operations, where attribution is almost impossible, would not be conducted by Russia or Russian operatives for morale concerns should be taken off the table.

Whether Western militaries like NATO Allies can create with its ongoing and floating ideas of a “Cognitive warfare concept”, a concept able to cope with Russia’s reflexive control theory, is seen by the author as sceptical. By copying it, it will be a value-based-subset only, which can’t create the Russian’s outreach. Additionally, Russia has implemented system-thinking in hybrid as well as conventional military thinking, and it is conducting military operations and targeting accordingly.

This fosters the need for a fast implementation of Multi-Domain Operations and re-thinking defence as a total defence by integrating non-military security providers and striving for societal resilience.

Over the last year, pundits have permanently analyzed and discussed possible scenarios for the outcome of Russia’s war on Ukraine. One of the constants in all scenarios was that hybrid threats and warfare would continue due to their cheap and, unfortunately, effective and flexible nature. The unexpected high conventional losses of personnel and material of the Russian military amplify the risks of hybrid threats in a post-war setting.

Whether Russia will win or lose the war, to bridge the time gap of regaining sufficient conventional military power, hybrid threats and warfare will be Russia’s first and cheapest choice to control, especially in the European geopolitical sphere. ■



DR. JOSEF SCHRÖFL



- ’ B.A. in Computer Technology, an M.A. in Intern. Relations from University of Delaware/US and a PhD in Intern. Politics from University of Vienna.
- ’ Deputy Director for Col Strategy & Defence, leading the Cyber-workstrand there
- ’ **Hybrid CoE Helsinki/Finland**



SOENKE MARAHRENS



- ’ Full Diploma in Computer Science, he holds a master’s degree from the Royal Military College in Kingston, Canada, and another from the University of the Federal Armed Forces in Hamburg.
- ’ Director, Col Strategy & Defence, leading the Hybrid warfare-workstrand
- ’ **Hybrid CoE Helsinki/Finland**



REFERENCES:

- [1] Lonas Lexy, "Here are Russia's alleged war crimes in the Ukraine invasion," The Hill, <https://thehill.com/policy/international/3262626-here-are-russias-alleged-war-crimes-in-the-ukraine-invasion/>.
- [2] Jack Peat, "War-torn Ukraine running more reliable train service than TransPennine Express," January 06, 2023, <https://www.thelondoneconomic.com/news/war-torn-ukraine-running-more-reliable-train-service-than-transpennine-express-342002/>.
- [3] Claire Parker, "Russia and Syria conducted dozens of illegal 'double tap' strikes, report says," The Washington Post, <https://www.washingtonpost.com/world/2022/07/21/syria-russia-double-tap-airstrikes-report-war-crimes/>.
- [4] Lew Gudkov, "Interview Conducted by Christina Hebel in Moscow," Der Spiegel, <https://www.spiegel.de/international/world/opinion-researcher-lev-gudkov-russians-have-little-compassion-for-the-ukrainians-a-066c08c6-60f4-48e1-853a-d2b3d67bd6b8>.
- [5] The initial assumption about the trustworthiness of the mercenaries was already raised during the Webinar on 14.02.2023.
- [6] "Seeing Red," Hybrid COE 8th Research Report, Jukka Aukia & Lucjan Kubica, March 2023, 34.
- [7] Former Research Director of Hybrid COE, Prof Dr Hanna Smith, in a "mind-opening" email exchange with the author.
- [8] Former Research Director of Hybrid COE, Prof Dr Hanna Smith, in a "mind-opening" email exchange with the author.
- [9] Former Research Director of Hybrid COE, Prof Dr Hanna Smith, in a "mind-opening" email exchange with the author.
- [10] Emmanuel Akinwotu, April 05, 2022, "Russian mercenaries and Mali army accused of killing 300 civilians," <https://www.theguardian.com/world/2022/apr/05/russian-mercenaries-and-mali-army-accused-of-killing-300-civilians>.

CRISIS COMMUNICATION STRENGTHENS RESILIENCE



Crisis communication aims to mitigate the impact of a crisis on the people involved. The aim is to communicate crisis scenarios and what is being done to rectify the situation from a situational picture.

In one way or another, the crisis shocks the human mind. A big crisis in a big way, a small crisis less. Everyone has their own personal relationship with the crisis. Crisis communication provides people with material and concepts to process what they have experienced and restore normality as soon as possible.

There are many types of crisis. An accident is one of the most typical crisis situations. The need for crisis communication only arises when its effects begin to affect individuals or entire stakeholder groups. Until then, it is a question of information flows related to crisis management and decision-making based on them, which are also absolutely crucial.

Crisis communication begins when people want to influence their thinking, experience, and actions. Then emotions, values and beliefs are at stake. The aim is to influence them by describing the situational picture and offering facts, but also by experiencing encounters, as this strengthens – or weakens – the ethos of those responsible for crisis communication.

This brings us to the heart of crisis communication. Ultimately, it is about strengthening feelings of security and control, i.e. the agency of those involved. On this ground rests individual and collective resilience. Problem situations are solved as part of crisis management, but the most unpredictable link in the crisis, human being, is guided by the right kind of communication.

CYBER TALKS ABOUT PEOPLE'S BASIC NEEDS

Another important group of crises is crises affecting living conditions. Among them are exceptional natural phenomena that affect infrastructure, various systems. On the other hand, infectious diseases can also bring systems and actors in society to their knees, as we have recently learned in a hard way.

For modern people, cyberreality is a living environment and circumstance, and disruptions quickly affect people's everyday lives directly and the various infrastructures of society, such as electricity, water, food, money and transport.

Disruptions can come from various errors or accidents, but especially recently problems have started to be caused to systems intentionally. The ongoing global political tension creates a need for actors to break the living conditions of others.

Regardless of the cause, disruptions and their threats return people to their basic needs. At the bottom of the hierarchy of needs are needs related to immediate vital functions and physical well-being. Next is safety and integrity.

Satisfying these needs immediately gives rise to a variety of thoughts and emotions that crisis communication aims to guide. Not to mention more sophisticated needs such as social needs, self-esteem and self-realization. All of these can be disrupted.

THE WHOLE ESSENCE OF A CRISIS COMMUNICATOR IS A MESSAGE

In demanding crisis communication, facts alone are not enough. Naturally, they are an indispensable tool. Research has shown that people's decision-making is influenced by their emotions more than we are often willing to believe. Fractions of facts are placed on the emotional basis largely based on how the provider of facts is trusted.

So we are talking about a classic element of rhetoric, ethos. The other two are logos (words and logic) and pathos (feeling). The ethos is strongest in the communicator's presence, i.e. body language, in which facial expressions, among other things, are decisive. Much of a person's body language arises from the unconscious, so it reveals the speaker's values and belief system. Therefore, the insides of the mind must be in order.

It is clear that a communicator representing authorities is expected to have a different appearance and body language than, for example, a representative of an organisation that has been the victim of a crisis, and who, as the head of crisis operations in his or her organisation, may also be a victim.

The form of care provided by a commercial operator may also be different from that of an authority. However, a person in crisis always expects to be cared for and that it is expressed verbally and with acts. It arises from our mental structure.

THE MEDIA REPRESENTS AN AUDIENCE THIRSTY FOR KNOWLEDGE

The media – both editorial and social – play a key role in crisis communication. Today, the communicating organisation has its own digital channels, various social media accounts and its own website. Their activity and relevance also guide the audience towards them.

In larger or more dramatic crises, traditional media also form their journalistic view of the situation. In crises involving people, the media follows the emotion at the heart of the crisis. That is its job. Therefore, the crisis communicator must also understand the logic of emotions and influence the reality of emotions.

It is always better if background relationships have been established with relevant media and journalists already in "peacetime". This makes it easier to get correct and enlightened information through the media in the midst of a crisis.

Reputation cannot be controlled, but the factors that make it up can be influenced through competent crisis communication. The reputation of the organization among the public is formed in the mind of each individual. Of course, it will be crowdsourced, where all kinds of media act as a platform.

CRISIS IS AN ABNORMAL STATE

A crisis is always an abnormal situation for those experiencing it. Otherwise, it would not even be a crisis. It's normal for a person in crisis to experience abnormal emotions. The aim is to get out of the situation and towards a normal life with as little trauma as possible.

Crisis communication means knowing and influencing the mental world of oneself and other actors. It needs to be practiced before a crisis strikes. The wording needs to be carefully considered, the performance in front of the camera repeated. This makes it more natural to act in crisis communication situations.

You can prepare for a crisis. Crisis communication principles, roles – above all, leadership – and clear instructions are essential. Their absence is pure foolishness. Creating scenarios of potential exceptional situations makes it significantly easier to initiate crisis communications once the situational picture has become clearer.

Crisis management aims to solve the problem itself. Crisis communication aims to achieve social acceptance of actions, to survive with as little reputational damage as possible and to strengthen the resilience of all stakeholders. ■



TANELI HASSINEN

Taneli Hassinen has worked as Communications Director at Finnair, SRV and Taaleri. In recent years, he has worked at Functos Oy e.g. as a crisis communications consultant.

ECONOMICAL IMPACTS OF DATA BREACHES

// Leo Taalas



Companies are increasingly using digital technologies in all facets, ranging from internal operations to customer engagement. Digitalization has brought with it significant improvements to processes, efficiency, and innovation, enabling companies to create more added value for their customers.

On the other hand, the digital transformation has also introduced significant risks and vulnerabilities. The expanding digital domain creates a broader attack surface for cyber-attacks; one potential threat are data breaches. Managing data properly has become a pertinent issue for companies trying to apply digital tools safely. Preparing against more frequent and complex cyber-attacks has become a strategic concern for companies.

A breach of sensitive data regarding proprietary information, customers or employees is likely to have a negative impact on daily operations, services, and revenues of a company. Reputation and stock price may also be affected by the announcement of a data breach. However, assessing the impacts of announcements of data breaches is not straightforward, as many direct and indirect variables need to be considered.

Interest in the effect of cyber-attacks on companies emerged in the wake of the 9/11 attacks of 2001. Mike McConnell, the former director of the US National Security agency, warned of a potential “Cyber 9/11” as a possible extension to the physical attack. The potential threat of a large-scale cyber-attack led to research to discern the significance for companies.

The majority of studies analyzing the impact of cyber-attacks on companies have utilized the event study methodology. In general, previous research has suggested a negative correlation between cyber-attacks and stock prices. Recently, there has been increased interest in analyzing the impacts of cyber-attacks across industries and at different time points.

My bachelors thesis completed in June 2023 for Bocconi University applies the market model event study – a variation of the event study methodology – to assess the impact of an announced data breach on stock price. The market model was built on a prediction period of 135 days of data prior to the announcement of a data breach. Event windows of $(-1,1)$ to $(-1,20)$ days were used in calculating cumulative abnormal returns (CAR) and subsequently cumulative average abnormal returns (CAAR). These measures give an indication of supernormal returns following an announcement of a data breach.

Analysis was conducted on a subset of incidents selected from the Privacy Rights Clearing House (PRC) data breach chronology. The analysis is conducted on publicly traded companies facing data breaches due to hacks. This results in a dataset of 63 data breach incidents spanning from 1/2/2005 to 7/2/2022. The NASDAQ and

NYSE stock and index prices used in the research are collected from the Refinitiv DataStream.

My analysis, firstly, used the cumulative average abnormal returns (CAAR) measure to assess the impact of data breach announcements on stock returns. The -1.8% CAAR indicates that the hypothesis of a negative relation between stock price and data breach announcements holds when considering the entire sample of 63 data breaches.

Secondly, the difference in effects caused by data breach announcements on stock returns between NASDAQ and NYSE listed companies was assessed. The results revealed a difference in stock price responses in companies listed on the NASDAQ and NYSE: the cumulative negative effect on incidents on NYSE listed companies was -1.3% at its maximum on Day +2, whilst no significant impact was found for incidents on NASDAQ traded companies. The result is likely due to operational differences – dealer vs. auction market – of the markets and the nature of the companies listed.

Thirdly, differences in impacts of data breach announcements on stock returns across industries was analyzed. Finance companies had the most pronounced negative impacts with a negative CAAR of 1.3% on Day +2. Comparing the retail sector to finance, there is a significantly smaller, but more immediate negative effect of -0.43%. The stronger reaction to data breaches in the financial sector may be due to the pivotal role of trust in the business model of financial companies. The results did not show a significant impact of data breach announcements on manufacturing, technology, and other companies. The insignificance of the impact could be in part due to a heterogeneity of companies in this group.

The results of this paper give indications of the effects of data breaches on companies. Understanding the current threat landscape, in terms of likelihood and cost, allows for the appropriate precautions to be taken by organizations to avoid devastating financial impacts. ■



LEO TAALAS

’ Analyst
’ Cyberwatch Finland



COULD ALL-OUT WAR FLAME OUT IN THE BALTIC SEA REGION?

// Timo Hellenberg

Russia's geopolitical ambitions in the European High North are on the rise. Leaked documents from the German defense ministry have revealed a terrifyingly plausible scenario for a full-scale Russian attack on the Baltic states and Poland. According to the report, the Putin regime could mobilize 200,000 new conscripts in February, while the Russian army quietly builds up forces on the borders of Poland and Lithuania. The first significant NATO forces to arrive would be Polish, after approximately 72 hours, but sizable German and other European NATO forces would not be seen for at least 10-15 days. With small NATO tripwire forces in the Baltics relying on reinforcements, the situation is dire. Finland would not have time to mobilize or push units toward Russia, leaving Russia free to keep its military units in the area unchanged.

In the scenario, on day one, the war begins with an intensive missile barrage on high-value targets. An echelon of armor, attack helicopters, and rocket artillery pushes through Northern Estonia-Narva and Tallinn towards Estonian North-West Coastal town, Paldiski. Simultaneously, battalion-size naval infantry landed in Tallinn harbor. In the south, a second echelon pushes northwestwards from Belarus toward Kaliningrad Oblast through Lithuania and then immediately turns south to confront NATO forces coming from Poland. Rear echelon forces mop up the Lithuanian defenses and resistance in the following days. Latvia is ignored and sits in the Kurland Kessel, the Courland pocket. Its army lacks the means to respond.

Before the actual land-invasion described in the above report, Russians would start "hybrid" influencing tactics, which can be exerted through economic influence, political influence, information influencing, cyber espionage, and military influence. These tactics include preferential trade agreements, rebate supplies of oil and gas, debt relief, credit, symbiosis between corrupt government and organized crime, trolling and manipulation, territorial violations, extension of military intelligence to

infrastructure, "earmarking" key personnel, and more. It's essential that businesses and governments around the world remain vigilant to these tactics and work together to mitigate their impact.

Russia's strategic combined or "hybrid" influencing tactics have been well-documented in its home country and neighboring regions. As we enter a new decade, it's clear that these same tactics have found their way into Russia's expanding global influence. One emerging weapon in Russia's toolbox is the pressure of lasting stress, which can be exerted through economic influence, political influence, information influencing, cyber espionage, and military influence. These tactics include preferential trade agreements, rebate supplies of oil and gas, debt relief, credit, symbiosis between corrupt government and organized crime, trolling and manipulation, territorial violations, extension of military intelligence to infrastructure, "earmarking" key personnel, and more. It's essential that businesses and governments around the world remain vigilant to these tactics and work together to mitigate their impact.

Alarming, Russian security services have detained an alarming number of foreigners and Russian nationals on allegations of working with foreign intelligence since launching its invasion of Ukraine in February 2022. This operational mode will intensify in the Russian regions which are considered (новые чувствительные зоны) such as Baltic countries and the wider Karelia. This trend will accelerate the deeper Russia sinks into the black soil of Ukraine. Russian intelligence is traditional and built primarily on human intelligence and systematized eliminations. Its weakness lies in its cross-sectoral activities, as different factions fight for the Kremlin's favor.

An other fresh geopolitical review commissioned by the European Commission suggests that this could lead to challenges to the region's prosperity and governance in the next few years. The "Arctic Safety and Security Cooperation - Review of Crisis Coordination and

Response Arrangements in the European Arctic and High North" (T. Hellenberg, P. Visuri, S. Milne, 2023) report produced by the Finnish research group Hellenberg International and the Irish Munster Technological University highlights the emergence of new geostrategic and geopolitical frictions in the European High North, with the Baltic Sea being a key logistical corridor under pressure.

The Hellenberg-MTU report underlines that Russia has been rebuilding fast its military capabilities and modernizing its regional military infrastructure in the AZRF (Arctic Zone of the Russian Federation) by using a 'double dual' approach: Arctic infrastructure is being used for civilian and military purposes (dual-use), while Russia is also blurring the lines between offensive and defensive intent (dual-purpose). Russia has also developed the Arctic-M satellite system to monitor the wider arctic region, including the Baltic and Barents Sea. Besides transmitting the weather data it also covers the situation information on exceptional situations.

Kremlin will likely encourage Beijing's attempts to shape the future of High North economic activities and governance. The long-term role of Arctic development in Kremlin's precision sight is uncertain, especially due to the complicated scenarios of future global commodities markets, our short-term prediction is that Russia will likely challenge the West on the High North governance and dominance. The question remains: what is Europe's level of resilience to respond to the above challenge, especially in a situation where we face it without the taken-for-granted alliances?


What about then our preparatory measures? The Atlantic alliance will certainly remain a pillar of security in Europe, also in the future. But it seems that especially the smaller East European states are finally awakening on their own contributions. Lithuania is planning to increase its defense budget to 3.5%. Will Germany take more responsibility not only for its own security, but also for the security of the Baltic Sea region? The deployment of the German brigade in Lithuania was pushed forward when German Defense Minister Pistorius visited Vilnius on 18.12. to sign a roadmap for the deployment of the German brigade in Lithuania. A total of 5,000 German soldiers will be transferred to Lithuania and technical details will be agreed during 2024 (incl. host country support services, funding and operations). The core of the brigade consists of five battalions incl. tank and artillery battalions. Poland's strong growth as a defensive power has a significant impact on the security of the entire Baltic Peninsula. Similarly, Finland's and Sweden's NATO memberships lay the foundation for a situation where the security of the entire Nordic region is in one hand. It must

be recognized, however, that NATO – like all intergovernmental organizations – has its own internal problems.

Estonia, Latvia, and Lithuania are taking their commitment to forklift the Baltic regional security to the next level with the establishment of a "Baltic Defense Line." This network of hundreds of bunkers and other defense installations along their eastern borders will create a mutual defense zone and a framework for joint use of weapons systems. As part of this effort, Estonia will allocate €60 million to construct 600 bunkers along its 294-kilometer border with Russia, each capable of holding up to ten people and designed to withstand a direct hit from a 152-millimeter caliber projectile. The Baltic development highlights these countries' -own- commitment to strengthening their comprehensive defense capabilities and working together to ensure regional security. Recently, the ECDI (Estonian Center for Defense Investments) signed a deal worth around 200 million euros to order both 4x4 and 6x6 vehicles from Turkey, which it will provide to its two infantry brigades. The first Turkish wagons are scheduled to arrive in Estonia at the end of next year, and all the rest during 2025. So coming back to the question, could all-out war flame out in the Baltic Sea Region? More important than considering its likelihood is to understand that it is time to pay more attention to strengthen the European defense industry alliances, supporting our own capabilities, instead of creating mutual competition and thereby letting competitors from across the Atlantic and some far-away exotic countries into our critical internal defense markets?

■



 **DR. TIMO HELLENBERG**
' CEO
Hellenberg International

CYBER SECURITY NORDIC WILL BE HELD AT THE END OF OCTOBER THIS YEAR

// Anu-Eveliina Mattila



The two-day Cyber Security Nordic (CSN) will be held this year at 29-30.10. in Helsinki Exhibition and Convention Centre and will once again gather top international speakers. Planning of the programme has begun, and ticket sales are moving fast. Registration for the event's pitching competition will open during March.

The event, organised for the sixth time, will focus on the latest trends, innovations, services and technologies in the cyber industry, as well as feature many international speakers and top experts in cyber industry appearing in Finland for the first time.

Cyber Security Nordic offers the latest information and trends, expert encounters, insights, networking and business opportunities. The event is aimed at cyber security professionals, organizational and corporate management, as well as experts responsible for information security and IT.

Anssi Rajala, who previously worked as Sales Manager of technology events at the Helsinki Exhibition and Convention Centre, has been appointed Business Manager of Cyber Security Nordic, after Marcus Bergström has taken over as Director of Events and Congresses at the Helsinki Exhibition and Convention Centre.

"Cyber Security Nordic is a unique top event in these latitudes, and we want to place more emphasis on the fact that companies and organisations of all sizes can get advice here on securing their own digital operating environment, reducing business risks and protecting intellectual property, update their awareness and find partners to take on these challenges," says Anssi Rajala.

The programme of the two-day event is planned in close cooperation with a programme group consisting of industry actors and strategic partners. Topical themes are explored from the perspectives of both companies and public administration. The discussions will focus on, for example: Europe's secure digitalisation and information security, cybercrime and law enforcement, democracy, cyber war and defence, geopolitics and cyber diplomacy. The event programme also discusses the latest solutions that support learning and competence development. By following Cyber Security Nordic on LinkedIn, you will receive information about the development of the event program and partners.



Cyber Security Nordic offers the latest information and trends, expert encounters, insights, networking and business opportunities.

CYBER SECURITY NORDIC COMPETITION OPENS IN MARCH

In the autumn, the finalists of the competition will again be selected, and they will be able to pitch for a prize of 10,000 euros at the event. The finalists will present their product or service in a pitching competition at Cyber Security Nordic, after which a professional jury will select the winner. The winner will receive a prize of EUR 10,000, which will be donated by the Finnish Fair Foundation (Suomen Messusäätiö). The competition was open to cyber security companies, teams or organisations operating and registered in Finland whose product or service meets one or more of the criteria of the competition.

The Cyber Security Nordic event is organised by the Helsinki Exhibition and Convention Centre in cooperation with the Finnish Cyber Security Industry Association Kyberala ry (FISC). The event's strategic partners are expected to be confirmed during the spring, when they will still have time to influence the planning of the event.

Cyber Security Nordic 2023 had a record 47 exhibitors and more than 1900 cybersecurity professionals from the private and public sectors. Top international and domestic talents gave topical presentations on two different stages.

Strategic partners included Accenture, HP, HSL Software, Huawei, Microsoft, Net Nordic, Nixu and Trend Micro. ■



ANU-EVELIINA
MATTILA

Anu-Eveliina Mattila works at the Helsinki Expo and Convention Centre and is responsible for the communications of the Cyber Security Nordic event.

FINNISH INFORMATION SECURITY CLUSTERS' APPLICATION GUIDE SUPPORTS COMPANIES IN COMPLYING WITH THE NIS2 DIRECTIVE

// Peter Sund and Risto Rajala

European Union NIS2 directive on measures for a common high level of cybersecurity was adopted in 2022 and replaced the previous NIS1 directive. The transposition of the directive into Finnish law is currently underway and the government is preparing a proposal for an act on cyber security risk management. The proposal is expected to be discussed in parliament during the spring and the application of the new act will begin already on 18.10.2024.

The aim of the NIS2 directive is to strengthen the common EU and the Member States' national level of cyber security focusing on sectors and actors considered critical to the functioning of society. This is accomplished by placing within the scope of the law mandatory risk management measures in the event of cyber security incidents. Risk posed by malevolent, illegitimate individuals and groups against the operation of information

systems, as well as the data stored in them, is still growing. Foreign, security and criminal policy measures based on international rules have so far not been able to sufficiently change the long-standing worrying trend. For this reason, it is still justified to focus on measures that enhance protection towards malicious actions.

From the point of view of the functioning of society, digital risk management measures of both the public sector and key private sector actors are at the heart of the directive. It is important to note that in Finland, the majority of digital infrastructure, information systems and data are held by companies.

The requirements of the NIS2 directive affect organisations operating in Finland in terms of business management, choices regarding technology and partnerships and operational control. Among other things, companies must regularly identify and evaluate cyber security risks in their

communication networks and information systems, implement risk management activities, maintain an incident management plan and report cyber incidents within the deadline and form. Organisations' acting management are responsible for arranging the implementation and supervision of cyber security in addition to approving risk management operating models and supervising their implementation. As a result of the regulation, the general responsibility of the management also extends to the previously separated task area of cyber security.

The upcoming Finnish Cyber Security Risk Management Act defines the actors covered by requirements of NIS2. Organisations are divided into essential and important entities based on the criticality of the operating field and the size of the organisation. Both essential and important actors are in principle subjected to same requirements, but essential actors are also targeted with preventative monitoring. In addition, sanctions are stricter for essential actors.

Obligations under the NIS2 directive to strengthen digital risk management safeguard the continuity of companies' business operations, which can be considered positive impact on profitability, especially in the long term. Fulfilment of obligations also entails direct costs for companies, but these losses work towards ensuring security of operations and are predictable in nature, as opposed to those costs associated with issues arising from mismanagement of digital risks. The realisation of risks typically causes unpredictable costs, both direct and indirect, which may also result in liability for damages, and, at worst, administrative fines already mentioned above. By going beyond the minimum requirements of the directive, a company can also gain a competitive advantage. Businesses will also benefit more broadly from the strengthening of society's cyber resilience and a more reliable and proactive operating environment, which will be positively affected by the directive.



PETER SUND

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

Kyberalariy. has, together with its members, drawn up the NIS2 Application Guide to help companies manage their overall security and help them meet their legal obligations. The members of an association representing the cyber security industry established in Finland started a joint industry-wide project to prepare a guide for the application of the NIS2 directive with the formation of a core group in autumn 2023. Dozens of companies from different segments of the cyber security industry have participated in the preparation of the guide. The cyber industry has actively followed the work on the NIS2 directive and influenced its content. The association strongly supports the objectives of the directive and is committed to doing its part to ensure its successful implementation.

Interpreting and complying with the new obligations may prove challenging for many companies covered by the directive. The application guide harnesses the expertise and experience of Finnish cyber security experts to support companies in need of help. The application guide explains the content of the new obligations in plain language and illustrates with practical examples the importance of managing digital risks and securing business continuity. The guide describes how the minimum requirements of the NIS2 directive set out by national law are implemented, using the most appropriate elements of the three widely identified information security management frameworks. The purpose is to illustrate the reasons for the requirements of the directive, describe the desired level of cyber security risk management and help companies to achieve a effective lower level of risk alongside compliance with the law.

A preliminary version of the application guide will be published in spring 2024, and the guide will be supplemented once the Act on Cyber Security Risk Management has been approved in its final form by parliament. The Finnish cyber security industry is ready to support companies falling within the scope of the Act in complying with the new obligations. ■



RISTO RAJALA

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



SAMPLES FROM CYBERWATCH FINLAND WEEKLY REVIEWS

// Cyberwatch Finland Analyst Team

THIS COMPILATION INCLUDES FOLLOWING ARTICLES

WEEK 5:

- Deepfakes and China cause worry in the US preparing for elections

WEEK 6:

- DDOS attacks losing impact

WEEK 8:

- Ukraine Won the Information War – Does it Matter?

WEEK 9:

- Tech giants fight disinformation in the EU, Digital Services Act affects in the background



DEEPFAKES AND CHINA CAUSE WORRY IN THE US PREPARING FOR ELECTIONS

U.S. security officials have raised concerns about outside interference in the upcoming presidential election this fall. Both the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) issued warnings in January. These concerns relate in particular to AI-based deepfakes, whose credibility is constantly evolving. If in the last presidential election the most ambiguity was caused by the contestation of the election results, the greatest threat in this election, according to the authorities, is the general chaos that deepfakes could cause.

Deepfake refers to a counterfeit that contains an video or sound that appears to be genuine and has been produced using machine-learning artificial intelligence. These are quite popular, and especially in TikTok and YouTube, one can find content, where politicians or celebrities are made to talk to each other about a wide variety of topics, such as video games. In the context of elections, deepfakes serve as a means of spreading mis- and disinformation and influencing the outcome of an election. Signals of the threat they pose in the United States were seen in January when, during the Democratic primaries, fake phone calls were used as a tool, in which the vote had been changed to that of President Joe Biden. This was used to conduct a phone call campaign in the state of New Hampshire, urging people not to vote at all. The impact of harassment remained unclear, but similar campaigns closer to the actual elections and spreading on social media, for example, could, at worst, affect voting behaviour.

In the United States, deepfakes have also raised concerns about possible foreign interference in elections. In particular, the speeches by the authorities have highlighted concerns about China and its enormous cyber

resources. Although China was not directly accused of making deepfakes, it was noted that it is an artificial intelligence superpower and the United States' most significant competitor in this field of technology. Chinese cyber influencing has recently been seen in connection with Taiwan's presidential election, for example, in the form of a large number of cyberattacks and fake news, so the threat must be taken seriously. However, focusing solely on China would leave many other players unchecked. The events that took place during the 2016 elections will certainly still be remembered. According to the report made afterward, the so-called Mueller Report, Russian special services actively seek to promote Donald Trump's election as president by, among other things, influencing social media, hacking various targets and publishing documents.

Deepfakes are not just a concern for Americans. In November in Slovakia, the far-right Republika Party used the voice of the leader of the Progressive Party in a deepfake as part of its election campaign. During the election campaign, there was also a high-quality deepfake of the same progressive party, in which, in a "secretly" recorded debate, there was talk of buying votes. Slovakia has a so-called electoral truce, which means that news coverage of elections must stop for a certain period of time before the vote. As a result, fact-checking in these cases remained in the hands of ordinary citizens and social media.

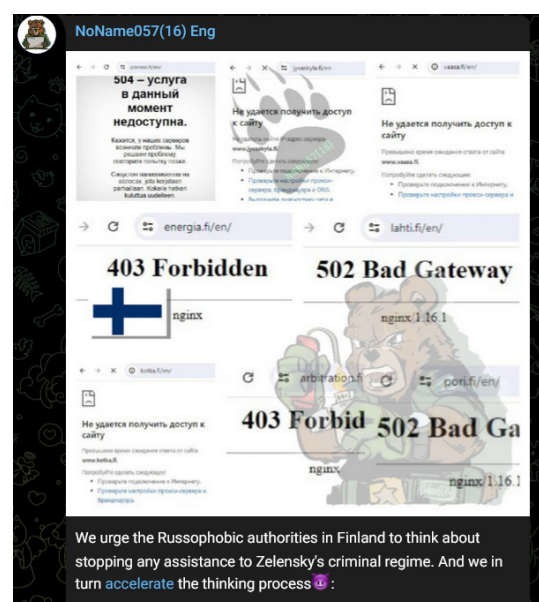
In the fight against mis- and disinformation, fact-checking, source criticism and good media literacy play a key role. If there are shortcomings in these, and especially if the media and social debate are polarised, as is the case in the United States, deepfakes can also sink into more fertile soil. ➤

DDOS ATTACKS LOSING IMPACT

In the first days of February, Finland experienced yet another wave of distributed-denial-of-service attacks, perpetrated by the already familiar Russian group NoName057(16). This actor, which considers itself a patriotic Russian hacker operator, constantly carries out these attacks on targets around the world. They are often timed to nationally significant days or moments when momentary service interruptions would receive as much attention as possible. In Finland, the attacks coincided with strikes in many sectors and demonstrations against government policies. The hacker group itself also stated that the reason for the attacks was "supporting the Finnish people against the actions of a government that pours money at the criminal government of Ukraine and abandons its own citizens." The attacks lasted for a couple of days until the group, as usual, moved on to the next country. On the third of February, the group's Telegram channel was already full of posts about France's criminal support for Ukraine and how the country's authorities and businesses will tremble under a wave of DDoS attacks.

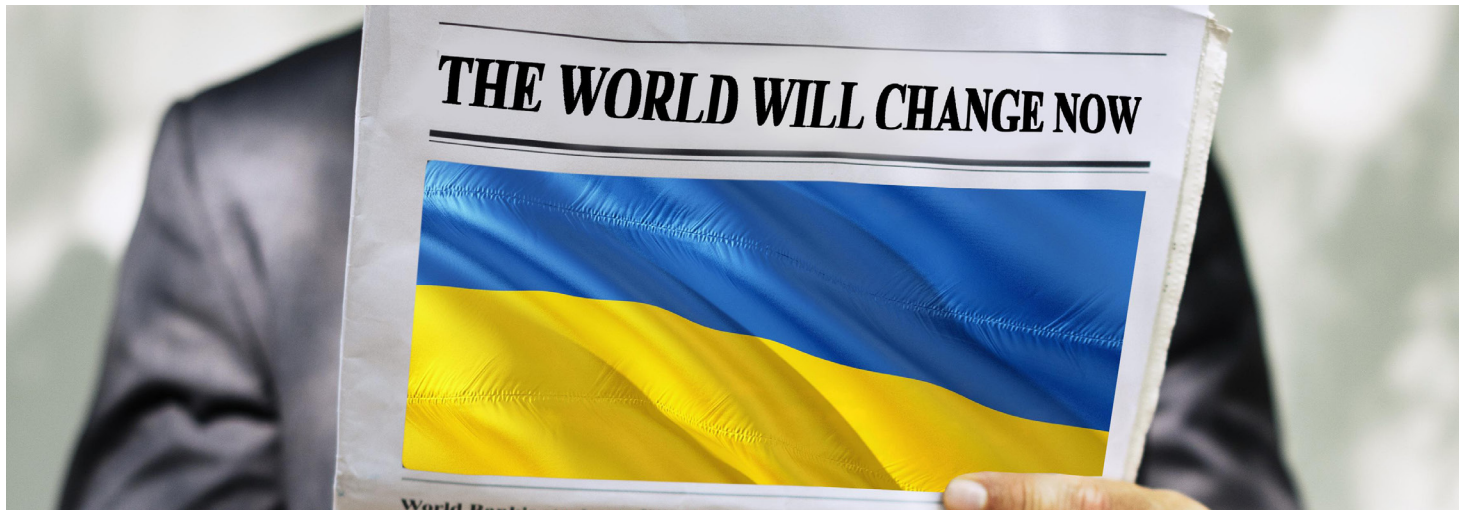
DDoS attacks are nothing new, and NoName's operations seem to have lost their effectiveness in Finland as well. The primary objective of attacks is to attract attention and increase national uncertainty, but it seems that DDoS attacks are already used to and understood as low-level interference as opposed to dangerous cyberattacks. Of course, the media picked up on the wave of attacks, but the news coverage was not sensational, but rather the style seemed to be to convey information about what is going on and what DDoS attacks mean. This is not only natural, but also important. Media has to highlight such a large wave of attacks, as a result of which the websites of several cities and major companies are simultaneously disrupted. Citizens should be kept aware of denial-of-service attacks, especially coordinated waves of attacks such as this one, even if the actual impact of attacks is both short-term and minor. If this would not happen, the attackers' objective could be much more successful when citizens would find that everyday services are not working without knowing what is really happening. It seems that Finland's national resilience to this threat has increased and denial-of-service attacks will not achieve the effect that the threat actor seems to want from them.

However, it should be noted that the value of denial-of-service attacks as a tool for influencing information is not only directed at the citizens of the target country. Especially in the case of a group that publicly announces its operations, such as NoName057, communication with those who support the group and its cause and followers of its social media channels is also essential. Pictures of the



targeted websites being down are posted rapidly on these channels and posts are full of descriptions of how the lives of the citizens of the target country are made much more difficult due to their actions. This will help maintain the impression that the West is constantly suffering from Russian cyberattacks, and possibly even encourage new hackers to join the patriotic cyber front. NoName057's Telegram channel also posts a lot of borderline false reports of attacks that in reality did not significantly affect the availability of the target service or were not even noticed in the target country. For example, in the last week of January alone, the same group had reported attacks on Finland in three different batches, allegedly targeting the National Cyber Security Centre, the Ministry of Justice and the Helsinki Chamber of Commerce, but these events did not even cross the news threshold in Finland. Admittedly, these most likely have been operations carried out with less intensity. This can also be indicated by the fact that no attempt was made to date them to socially significant moments. Still, the group announced them on their channel with the same boisterous energy as the attacks in early February.

However, DDoS attacks are not entirely harmless. They can also cause real harm if they can be timed at times when access to information about the targeted services would be very critical. For example, DDoS attacks timed to coincide with crises or other exceptional events may be effective in promoting uncertainty, even if we know exactly what they are about. Although in general they do not pose a significant threat, one should not be lulled into an apparent sense of security or the idea that one is completely protected from influence. Attacks should be understood in many different ways as a tool that serves the objectives of information influencing. They are unlikely to disappear from the cyber environment of Finland or Western countries, which is why we must both get used to them and prepare for them. On the positive side, however, the impact of attacks is constantly diminishing as organizations develop their ability to maintain operations when attacked, and citizens become more aware of what attacks are about.



UKRAINE WON THE INFORMATION WAR – DOES IT MATTER?

Information warfare is a central part of every modern conflict, including the war in Ukraine. The means of information influencing aim to influence the outcome of an ongoing conflict. Information influencing refers to activities that aim to systematically influence public opinion, people's behaviour and decision-makers. The goals include supporting one's own agenda or, alternatively, fomenting mistrust in the target society. Furthermore, information influencing can take the form of individual actions or extensive influencing campaigns, for example through botnets, social media or other means of communication. This can manifest itself, among other things, in the dissemination of false or misleading information and in presenting information that is correct in itself in a way that supports false narratives.

Ukraine can be considered to have defeated Russia in information warfare, at least in the West. An example of this is the dominance of narratives and perceptions presented by Ukraine, which can be seen to have triumphed over the alternative course of events presented by the Russians. Especially in the early stages of the war, Ukraine's strategic communication was particularly successful. War-related stories and memes spread around the world. Similarly, Russia has failed to spread its own narrative. Before the war, there was much fear of Russia's information weapon and trolls, but their impact both in Ukraine and in the West has remained limited. Despite the contradictions in attitudes towards Ukraine and Ukrainian refugees, Europe has even been disconcertingly united in its support of the country. Ukraine's successful communications and Western media, which have clearly supported Ukraine in the war, play an important role in this. Of course, when it comes Russia's information influence one must remember that it is not necessarily meant to convince the West, but the target group is its own citizens and countries outside Europe.

On the other hand, there are indications that Russia controls its own information space relatively well, and neither Ukraine nor the West is able to influence Russian

citizens. There has been no major anti-war movement in the country, despite attempts at informing Russian citizens, although the nature of an authoritarian society and sanctions for protesting certainly play a role in this. However, the Russian information space is also indicated by statistics from the research center Levada, according to which the amount of support for Putin has increased during the war, while attitudes towards the West have deteriorated. Although statistics from Russia should always be treated with caution, Levada has traditionally been considered one of the most reliable sources of information in the country. In this light, Russia's information influencing directed at its own citizens seems to have been successful. On the other hand, for those Russians who want independent information, such would certainly be available, for example, from independent Telegram channels and opposition media often operating abroad. However, there is a considerable threshold for obtaining information openly from sources opposed to one's own regime, and it is extremely easy for the Russians to simply turn a blind eye to the war. It is virtually impossible for Ukraine to penetrate and gain a foothold within this information wall, and it is unlikely that Russia will lose control of the narratives within its own borders.

Information warfare is constantly taking place. Although Ukraine has already won Western hearts, the country is also waging a kind of consumer war in the information environment. Recently, Western media has also featured more news than before about Ukraine's challenges, such as the shortage of personnel and ammunition. The possibility of defeat for Ukraine and the need for peace have also been seen here and there. Ukraine's challenge is to maintain its own narratives and war in people's minds as topical, important and international. At home, it is critical to maintain the morale of citizens, faith in victory and support for the continuation of military operations. In the end, the key question is how Ukraine will succeed in transforming information domination into concrete domestic and Western support. Winning the information war is of no comfort if on the physical battlefield only a silver medal is on offer. ➤

TECH GIANTS FIGHT DISINFORMATION IN THE EU, DIGITAL SERVICES ACT AFFECTS IN THE BACKGROUND

The anti-disinformation front in Europe received new reinforcements in February when Google and Meta announced that they would launch campaigns to combat disinformation in the context of the European parliament elections in June. In particular, the EU has feared an increase in Russian propaganda and its impact on the upcoming elections. The companies' announcements symbolically coincided around with the start of national application of the European Union's Digital Services Act (DSA), which was on 17th of February. It has been hoped that the DSA will contribute to the fight against disinformation by imposing obligations on online platforms, including on platform moderation, and by obliging platforms to assess and mitigate risks related to democratic and electoral processes. DSA's obligations have already applied to very large online platforms and search engines since 25 August.

In Google's case, the company will launch an advertising campaign between April and May in different platforms, including YouTube and TikTok, in five EU countries: Belgium, France, Germany, Italy and Poland. The advertisements contain information on how to identify misinformation and disinformation and what kind of misinformation is sought to spread. The campaign uses so-called "prebunking" methodology. This means that the aim is to get the target notified of false information earlier than the false information itself reaches the target. When such misinformation reaches the target, he already knows to take it with caution. The reasons given for choosing these countries as the target for advertising included an opportunity to reach a large number of voters in the elections and to make use of the company's own local knowledge. Although the campaign targets the EU's most populous countries, it excludes a significant number of eligible citizens from other member states, which contributes to weakening its effectiveness. However, these measures are undoubtedly appropriate and heading in the right direction.

Meta, meanwhile, is addressing the problem by opening a dedicated Elections Operation Center to identify and counter threats in real time. Tackling misinformation includes fact-checking with 26 partners across the EU in more than 22 languages. In addition, the aim is to tackle coordinated influencing operations and respond to possible misconduct with artificial intelligence, such as deepfakes.

Both companies' decisions are certainly partly influenced by the EU's Digital Services Act, although the announcements do not directly refer to it. According to the European Commission, the main objective of the act is to prevent illegal and harmful activities online and combat the spread of disinformation. However, the DSA has so far received more public attention for its obligations to allow platform users to opt out of personalised marketing, the obligation to create easily understandable terms of use, the obligation to moderate content more openly and the possibility to appeal against the moderation decision. In addition, the DSA unequivocally prohibits targeting advertising at children and targeting advertising at adults on the basis of, for example, ethnic background or sexual orientation. The aim is therefore to increase users' rights and influencing opportunities.

Although the act itself applies to virtually all digital services, it focuses on very large online platforms and search engines. By definition, this includes services whose monthly number of active users exceeds 45 million users in the EU area when examining the average for a six-month period. For these very large operators, an additional obligation is to assess four distinct risk categories, for which measures should also be taken to reduce risks. These include risks related to the dissemination of illegal content, such as the spread of illegal hate speech, democratic processes, civil dialogue and electoral processes. The maximum amount of fines for non-compliance with regulatory obligations can be up to 6% of a company's annual worldwide turnover.

EU regulation is often described as bureaucratic and its achievements are doubted. However, it is clear that it also has positive effects. DSA is possibly an example of successful regulation from the citizen's point of view, as it increases the transparency of services and users' choices regarding their own privacy. For wider society, the benefits can be seen precisely in the form of the campaigns described above, which can contribute to reducing the effectiveness of attempts to influence the EU by hostile actors. ■





REFERENCES

DEEPPAKES AND CHINA CAUSE WORRY IN THE US PREPARING FOR ELECTIONS:

<https://cybernews.com/news/fbi-nsa-cybersecurity-election-interference/>
<https://www.cnn.com/2024/01/10/how-fbi-nsa-are-preparing-for-deepfakes-ahead-of-2024-elections.html>
<https://faktabaari.fi/fakta/presidenttiehdokkaiden-puheita-on-kloonattu-ja-muokattu-tekoalilla/>
<https://www.justice.gov/archives/sco/file/1373816/download>
<https://www.nbcnews.com/politics/2024-election/fake-joe-biden-robocall-tells-new-hampshire-democrats-not-vote-tuesday-rcna134984>
<https://www.nbcnews.com/tech/misinformation/joe-biden-new-hampshire-robocall-fake-voice-deep-ai-primary-rcna135120>
<https://www.politico.eu/article/china-bombards-taiwan-with-fake-news-ahead-of-election/>
<https://yle.fi/a/74-20056699>
<https://yle.fi/a/74-20071490>

DDOS ATTACKS LOSING IMPACT:

<https://t.me/s/noname05716eng>
<https://www.hs.fi/talous/art-2000010202403.html>
<https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-jatkuvat-mynos-vuonna-2024>

UKRAINE WON THE INFORMATION WAR – DOES IT MATTER?:

Cyberwatch Finland Weekly Review Week 8/2024

TECH GIANTS FIGHT DISINFORMATION IN THE EU, DIGITAL SERVICES ACT AFFECTS IN THE BACKGROUND:

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_fi
<https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops>
<https://digital-strategy.ec.europa.eu/en/policies/dsa-impact-platforms>
<https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32022R2065#d1e2324-1-1>
<https://faktabaari.fi/nakokulmat/nakokulma-digipalvelusaados-lisaa-avoimuutta-ja-vahvistaa-kayttajien-oikeuksia/>
<https://prebunking.withgoogle.com/>
<https://blog.google/around-the-globe/google-europe/supporting-elections-for-european-parliament-2024/>
<https://about.fb.com/news/2024/02/how-meta-is-preparing-for-the-eus-2024-parliament-elections/>

MONTHLY REVIEW

JANUARY 2024

// Cyberwatch Finland Analyst Team

CONTENT:

1. EVENTS IN THE CYBERLANDSCAPE OF 2023
 - 1.1 International Cyber Environment
 - 1.2 Cybercrime
 - 1.3 Technology
2. OUR HIGHLIGHTS OF 2023
 - 2.1 How cyberwar developed in 2023
 - 2.2 The Rise of Hacktivism
3. FOLLOW THESE ALSO IN 2023
 - 3.1 NIS2 - Act on Cyber Security Risk Management coming soon
 - 3.2 Critical infrastructure continues to attract interest



IN THE MONTHLY REVIEW

In this monthly review, we examine the most significant cyber phenomena of the previous year, tying them into larger concepts. The review is divided into three perspectives: continuous monitoring targets, phenomena that we want to highlight especially from the previous year, and phenomena whose development is worth monitoring going into 2024.

With regard to the international cyber environment, it is worth noting that in 2023 it still appeared as a ruleless, even anarchist state. This is evidenced by, among other things, the spread of conflicts into the cyber world, the impact of attacks on civilians and the lack of international legislation. Both the EU and the UN have sought to extend their influence in the area of cybersecurity, but there is still a long way to go before common global rules of the game are created.

As new technology and new forms of crime became more effective, cybercrime became more effective. Cybercrime also became increasingly important in interactions between states, and the boundaries between

organised crime in the physical world and cybercrime became increasingly blurred.

By far the most significant phenomenon in technology in 2023 was the disruption created by the spread of artificial intelligence technology. The number and potential use of various AI applications grew exponentially, and they were useful both in promoting cyber security and in enhancing criminal activity. However, the development targets in the field of technology were not limited to artificial intelligence, but competition for microchip production capacity between the United States and China, for example, remained fierce.

Among other phenomena this year, we would like to highlight the development of cyber war in the conflict between Ukraine and Russia and the role of ideologically motivated cyber activists, i.e. hacktivists. Among the significant changes next year, we highlight the requirements created by the NIS2 Directive and the growing cyber threat to critical infrastructure.





1. EVENTS IN THE CYBERLANDSCAPE OF 2023

1.1. International Cyber Environment

The year 2023 could be described as the year of international anarchy in the cyber world. The term used in the study of international relations refers to a situation where the world lacks a supreme authority or sovereignty that could settle disputes, enforce the law or organize the international system. The metaphor is also apt in the cyber world. During the year, the spotlight has been on several different crises: the war visible in the Ukraine-Russia cyberspace, the US-China trade war, for example sanctions on microchip technology, and cyberattacks carried out by volunteer hackers and hacktivist groups in various conflicts. The cyber environment appeared to be a chaotic grey area without rules.

Last year, cyberattacks increasingly affected ordinary citizens, not only in war-torn Ukraine. For example, at the NATO summit in the summer, public transport in the host city of Vilnius was hit by cyber attacks, which also affected the lives of ordinary people. The event doesn't have to be directly political either: France, the organizer of the upcoming Summer Olympics in Paris has expressed concern about a possible increase in the number of cyberattacks during the Games.

A solution to the anarchy of the cyber world is unlikely to be forthcoming, even though attempts were seen during 2023. Last year, the EU, in particular, excelled in regulating the cyber world. The aim is the Brussels effect, which refers to the phenomenon of the adoption of regulations drawn up by the European Union in other

parts of the world. For example, the data transfer agreement approved with the United States in the summer, the Chat Control initiative that worried privacy activists in the autumn, the NIS2 cyber security directive and the artificial intelligence regulation currently under way are significant, even though there are no guarantees that they will spread globally. The United Nations has also sought to take the lead: a cybercrime treaty that has been in preparation over the past year may see the light of day in 2024. The agreement would aim to facilitate the sharing of information between states and to form a common understanding of what cybercrime means. The agreement has faced headwinds, with sources saying that the negotiating countries are divided into blocs with authoritarian states on one side and Western countries on the other.

The inability of states to secure cyberspace or regulate anarchy in it has been striking. If the EU, the UN or states in other frameworks are unable to bring order to the cyber world, initiatives from other actors will emerge as an alternative. For example, in October, the International Committee of the Red Cross published a list of eight rules for civilian hackers conducting cyber operations. For the time being, it is too early to say how well the rules will be complied with, or whether they will be complied with at all, but this is an opening in the right direction. In the absence of universal cyber laws, a possible development is an even more drastic blockade in allied circles. The sharing of threat intelligence and defence cooperation is already clearly limited within alliances.



1.2. Cybercrime

In 2023, the term that best describes cybercrime is constant change. Over the past year, we experienced this in several ways. Whether it's the introduction of new technology, the development of operating methods or completely new types of crime, a new aspect of cybercrime emerged almost every week last year. On the other hand, this should come as no surprise, as the phenomenon has been changing practically throughout its existence, always evolving according to the ability of victims of crime and authorities to respond to existing practices. Significant changes in cybercrime are usually not so much completely new forms of activity, but the development of existing methods in an increasingly challenging and unpredictable direction. In many ways, we are already familiar with crimes as such, but the tools or methods used to carry them out are only evolving.

A good example of this is the development of ransomware attacks. A trend in extortion attacks, which started earlier but was highlighted especially last year, was that instead of or in addition to simply holding stolen data for ransom, criminals increasingly threaten victims with leaking the data or selling it for the highest bidder. These forms of attack, known as double or triple extortion, subject the victim to be ransomed through several different threats, and also often on many occasions. This type of attack has evolved in response to the fact that organizations have often prepared for blackmail with data backups or backup systems, so blackmail by extorting data alone is ineffective. On the other hand, the phenomenon is also supported by the increased reputational damage associated with cyberattacks and interdependencies

between organisations. If a company is the victim of a cyberattack and the stolen data is published, it can be difficult to convince partners that nothing related to them has been leaked, let alone earn the trust of new potential partners.

Another example of the evolution of crime can be found in phishing, which has been one of the most effective and popular forms of cybercrime for years. Last year, phishing as such did not change in any way, as its objectives and principles remained exactly the same. However, with the help of new technology, especially artificial intelligence, and new kinds of targets and means made operations more efficient and difficult to detect. Phishing messages evolved to be more credible, new ways of pressuring victims were found, and operations expanded as message distribution and translation into multiple languages became easier and cheaper.

In 2023, cybercrime changed mainly due to the development of existing forms of activity. At the same time, however, the activities became more organised and organised. The boundaries between cyber crime and organized crime in the physical world, or state operations, became increasingly blurred. Cybercrime is extremely lucrative and growing in importance every year. It is very likely that 2024 will also see developments in the implementation of existing cybercrimes, and there will certainly be many surprises when criminals come up with even more new ways to trick people or circumvent technical protection of systems.

References
on page
41





1.3. Technology

In terms of technological development, one cannot talk about 2023 without mentioning the exponential popularity and applications of AI. This is not only the most significant change in the field of technology last year, but possibly even the decade, or at least the beginning of one. Over the past year, various AI-enabled applications and systems became much more common, and more sophisticated AIs became available to a wider audience. This can be considered to have started already at the end of 2022, when the first AI application to receive massive attention, ChatGPT, was released for free use. As a result, both interest in artificial intelligence and, in particular, applications for generative text-generating AI such as ChatGPT were constantly being invented. These applications were developed for both well-meaning purposes, such as search machines or coding, but at the same time, criminal activities also developed, for example, in terms of phishing messages or searching for security vulnerabilities. There were also significant problems with the tools, such as plagiarism and copyright. Attempts were made to prevent the misuse of both ChatGPT and other AI applications by modifying the application according to the criminal uses that were invented for it, but this was rarely successful, as malicious actors either found ways to bypass restrictions or developed completely unrestricted proprietary applications based on the same technology. It is good to understand that with the advent of a new wave of technology, it is practically impossible to limit its use to legal or morally acceptable activities, as criminals will always find a way to exploit it.

During the past year, we got a taste of the potential of artificial intelligence in the form of both the promotion of cyber security and the development of the activities of threat actors. Artificial intelligence was successfully

utilised in cyber defence in automating cyber security monitoring, identifying errors in code and for criminals use was found for example in creating more credible phishing messages. In addition to security experts, the assessment of weaknesses in the code also served as a tool for criminals, as artificial intelligence does not know whether the gaps it finds in information security will be patched or exploited in an attack. Although the various applications of artificial intelligence that became common last year are already well developed, it is to be assumed that we are still at an early stage with the benefits of AI and the significance of the technology. At present, AIs are still relatively limited to only one type of activity, for example, text-generating generative AI cannot defeat humans in chess games or create credible videos or images, even though these are all functions in which AI can be effectively utilized.

Even though artificial intelligence took most of the attention in the field of technology, it should not be forgotten that there were also changes on other fronts. The competition for microchips and supremacy of future technology continued between the United States and China, and Russia faced increasing difficulties due to trade sanctions and disengagement from Western technology. The dependence on technology that the great powers are trying to spread around them is still a significant phenomenon. As information technology continues to play an increasingly important role in the functioning of societies, those who control the production of microchips will have a significant position of power in the field of international politics. At the moment, it seems that the United States is on top of the chip war, but in the future, the ability to develop quantum technology or artificial intelligence applications, for example, may shape this position.



2. OUR HIGHLIGHTS OF 2023

2.1. How cyberwar developed in 2023

There has been a lot of talk about cyberwarfare and how to define it, especially since Russia invaded Ukraine in 2022. In addition to ground battles, Russia also stepped up aggression in the cyber and information dimensions. During 2023, cyber warfare continued to be active and took on many new dimensions, both in Ukraine and around the world. The year 2023 showed, at the latest, how cyberwar is still a difficult concept to define, because cyberspace does not really recognize any national or other borders. This has also materialised as a challenge to hold cyberwar criminals accountable.

In the information dimension, cyber warfare is fought especially over alliances, credibility and mental superiority. Information operations and cyberattacks aim to influence, for example, how the civilian population perceives the ongoing physical war. The great powers use the information dimension to justify their own actions and to make the actions of other great powers appear in a bad light. In 2023, cyber warfare has also included a kind of arms race culture, where the cyber capabilities of one's own state have been publicly highlighted. An example of this is the United States, which visibly announced that it has increased the role of its digital combat forces against influence efforts from outside the country. China, on the other hand, was reported to have developed a new kind of satellite-intercepting cyber weapon, which naturally forces other major powers to rise to this challenge. China has placed great emphasis on how the information dimension, in particular, plays a key role in the country's military strategy and in countering foreign influence from its online environment.

In cyber warfare, targets and forms of action vary from cycle to cycle. As in physical warfare, there are often preparatory phases of varying lengths between active periods in cyber warfare. In the war in Ukraine, for

example, in 2023, both sides had time to learn about the other side's operating methods, which in turn forced the other side to modify its attack methods also in the cyber environment. The cyber war between Russia and Ukraine also emphasised the use of various external actors. In new forms of cyber warfare, the execution of attacks has been extensively outsourced not to the armed forces and authorities but to cybercriminal groups separate from the administration, which are able to activate very quickly. The use of various criminal groups and ideological hacker groups in cyber warfare often saves the use of the state's own cyber weapons for the most critical targets and more precisely planned attacks.

Hybrid warfare in general has increased globally, as evidenced by the growing number of cyberattacks also against states that have not directly joined any military operations. China, for example, also sees cyber power as a key part of its hybrid warfare concept, and many of its recent cyber operations can be seen as preparations for the Taiwan operation. It is likely that a significant amount of the most sophisticated state cyber activity is still taking place behind closed unknown to the public. There is also a lot of state-led cyber espionage and information gathering operations in the background that are not publicised. One of the changes in cyber warfare has been the attitude of states towards cyberattacks against the country, which efforts were made to respond more quickly in 2023. This has naturally increased the risk that cyber influencing will be responded to on the basis of the first assumption, without full certainty about the perpetrator. This, in turn, can increase the number of conflicts at least in cyberspace. In the future, increasingly planned kinetic military operations and terrorist attacks will also involve the use of cyber power.

References
on page
41





2.2. The Rise of Hacktivism

During 2023, the role of hacktivist and ideologically active groups as cyberattackers has become even more pronounced. This has also been reflected in the war in Ukraine, where crowdsourcing has taken steps forward. On the Ukrainian side, the warring It-Army of Ukraine has continued its activities and coordinated, among other things, denial-of-service attacks against Russia, while on the other side the same has been done by pro-Russian hacktivists.

The situation is not limited to the war between Ukraine and Russia, as Indian cyber volunteers, for example, have carried out attacks for political reasons. The role of volunteers has also been seen in the Gaza war, where both sides have received voluntary support. The main rule seems to be that in modern conflicts, be it political, diplomatic or military, voluntary ideologically motivated aggressors will also participate. There is also statistical evidence for this. According to a study by cyber analytics firm CloudSEK, the number of ideologically motivated cyberattacks accounted for up to 35% of cyberattacks between April and May 2023. The change has been rapid, as globally they were estimated to have

been only 1% in 2021. Although the figures should always be viewed with healthy suspicion, the increase in ideological attacks is acknowledged and observed by many experts.

Popular methods of attack by hacktivists and ideologically motivated attackers have been denial-of-service attacks and defacements of websites. These are relatively low-level activities, but the situation may change, as cooperation between factions can grow and thus become more dangerous and advanced. Organizing and recruiting like-minded people is easier than ever today. If for years hackers have been imagined to operate mainly on the dark and deep web, in 2023 publicly available channels, especially Telegram, gained popularity as a tool for communication and coordination of activities for cyber-criminals and hacktivists. Hacktivism seems to be here to stay, and the development of technologies such as artificial intelligence will probably make it easier for volunteers and those less technically skilled to participate in cyber battles. In the future, therefore, an increase in both low-level operations carried out by hacktivists and more complex joint operations can be expected.



3. FOLLOW THESE ALSO IN 2023

3.1. NIS2 - Act on Cyber Security Risk Management coming soon

The implementation of the NIS2 Cyber Security Directive into national legislation is being carried out at an accelerating pace. The Act on Cyber Security Risk Management will enter into force in October 2024. Organisations falling within the scope of application of the Act must register with the list of operators maintained by the supervisory authority by 1.1.2025. In the public sector, the implementation of the Directive will be handled by amending the Information Management Act.

As a result of the Act, operators will have a general risk management obligation for cyber security. Operators must identify, assess and manage risks by implementing adequate safety and risk management measures. The management is responsible for implementing the risk management operating model. As a result of the Act, organisations covered by the Act will also be obliged to

report significant deviations to the supervisory authority without delay. Failure to comply with risk management and reporting obligations and registration on the list of operators may result in an administrative fine.

It is worth starting the law now at the latest. It takes time to create a risk management model or improve an existing management environment to take cyber security into account. Similarly, meeting the minimum requirements for cyber risk management measures defined by law is a project that requires careful planning and determined work. A concrete start in the implementation of the ten minimum requirements can be achieved with a gap analysis that takes into account the law and the relevant frameworks (ISO 27001, cyber indicator).

**References
on page
41**





3.2. Critical infrastructure continues to attract interest

Growing concern about cyber threats towards critical infrastructure was present throughout 2023 more than ever before. Cyberattacks and attempted cyberattacks on critical infrastructure increased significantly. Attacks with which had a wide impact and gained a lot of attention were seen significantly more than before. This included several internationally significant ports and healthcare units, which were increasingly targeted by denial-of-service attacks and ransomware attacks, among other things. In Finland, too, the matter became concrete at the latest with the sabotage of the undersea telecommunications cables in the Baltic Sea and the gas pipeline between Finland and Estonia.

In many ways, critical infrastructure remains an attractive target for cyber influencing. The broad impact of attacks or the resulting disruptions on society as a whole attracts both financially motivated criminals and state actors, who may often also cooperate with each other. State influence may have been hidden behind a seemingly criminal or economic motive. Even in the cyber world, attacks on critical infrastructure have a very rare opportunity to cause significant physical damage, and the ripple effects of attacks are not limited to partners or customers. For example, an attack on the electricity grid or public transport also has considerable information impact value, which can serve ideological goals in sowing uncertainty and fear. Attacks are also often timed at a time that has the greatest impact on the target society.

During 2023, attacks on critical infrastructure could be linked to many broad-spectrum hybrid influence cam-

paigns, especially by Russia. State actors often seek to cripple critical functions of society as part of these hybrid operations. Cyberattacks targeting the energy sector, in particular, have been linked to hybrid warfare and state activities. Attacks on the healthcare sector also increased, especially as it is one of the most critical sectors of society. Healthcare is also a financially very profitable target for cybercriminals. In addition to the energy, logistics and health sectors, the media sector and law enforcement agencies have become significant new targets. For example, attacks on the media sector may aim to influence the information space and spread possible fake news. In addition to Russia, China and North Korea have been active state actors in recent years.

Often, attacks on critical infrastructure also have numerous ripple effects on other areas of society. The interdependencies of the cyber world are a theme that has been talked about for years. This means, for example, situations where disruptions in the cyber world spread effectively across organisational and cross-industry boundaries. A subcontractor can be used as a vector to achieve a broad impact, and instead of the company's own data, the ransom demand may be the interruption of the service provided to customers and the resulting harm. The effects of disruptions caused by attacks can also spread unintentionally, and attacks experienced by nationally significant actors in particular are widely felt. Cyberattacks on critical infrastructure will certainly increase in 2024 as well, and there is no doubt that attack methods will become more diverse and efficient. ■



REFERENCES

INTERNATIONAL CYBER ENVIRONMENT:

Cyberwatch Finland 2023 Weekly Reviews of year 2023

CYBERCRIME:

Cyberwatch Finland 2023 Weekly Reviews of year 2023

What is triple extortion ransomware? | Definition from TechTarget
WS_Professionalisation_of_CyberCrime_EN.pdf (withsecure.com)

TECHNOLOGICAL DEVELOPMENT:

Cyberwatch Finland 2023 Weekly Reviews of year 2023

HOW CYBERWAR DEVELOPED IN 2023:

Cyberwatch Finland 2023 Weekly Reviews of year 2023

THE RISE OF HACTIVISM:

Cyberwatch Finland 2023 Weekly Review, week

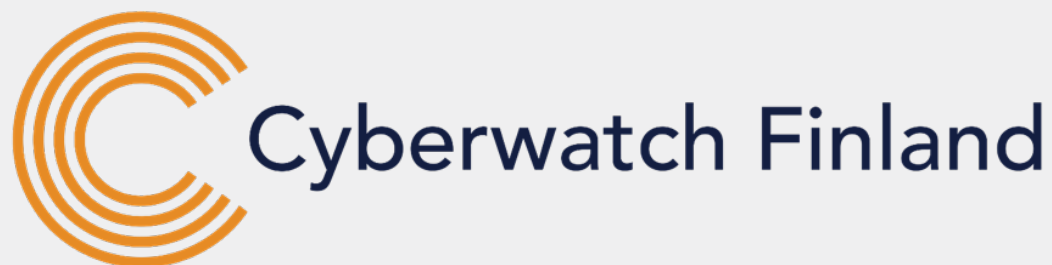
NIS2 - ACT ON CYBER SECURITY RISK MANAGEMENT COMING SOON

NIS2-directive (EU) 2022/2555

Hallituksen esitysluonnos eduskunnalle kyberturvallisuudirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

CRITICAL INFRASTRUCTURE CONTINUES TO ATTRACT INTEREST:

Cyberwatch Finland 2023 Weekly Reviews of year 2023

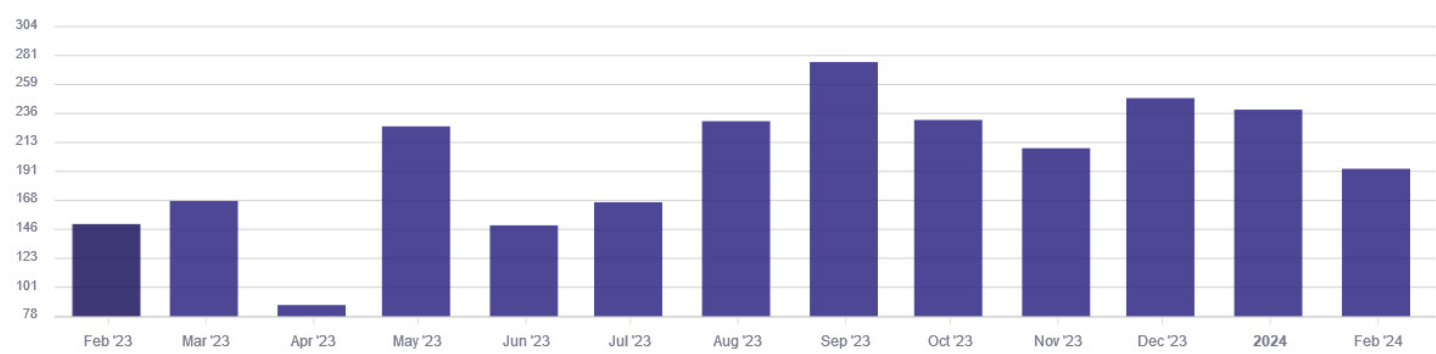


THREAT INTELLIGENCE REVIEW

Cyberwatch Finland publishes threat intelligence monitoring that collects the most significant cyberattacks of the past month and information on the most active 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.



DATA BREACHES BY MONTH FROM LAST TWELVE MONTHS.



Source: Cyber Intelligence House



MAJOR CYBERATTACKS AND CAMPAIGNS

LURIE CHILDREN'S HOSPITAL CHICAGO

DATE: 31.1.2024

DESCRIPTION: Lurie Children's Hospital in Chicago suffered a cyberattack by ransomware group Rhysida at the turn of January and February. The hospital is the leading pediatric acute care facility in the United States and treats more than 200,000 children annually. Attackers claim to have obtained 600GB of data and ask for 60 Bitcoins as ransom. At the time of writing, BTC is worth around €58,000, meaning the ransom is worth around €3.5 million.

ACTOR: Rhysida

MOTIVE: Economic

IMPACT: The hospital's IT systems had to be taken offline and some treatment procedures had to be postponed. Doctors had to switch to pen and paper when writing prescriptions. Now, about a month after the attack was detected, the hospital's IT services are still partially down and service disruptions are affecting some operating segments. Prescriptions are still handwritten, and some patient appointments have to be cancelled and rescheduled to make way for the most acute cases. The ransom demand is still active.

MAJOR CYBERATTACKS AND CAMPAIGNS

BJUV MUNICIPALITY

DATE: 24.1.2024

DESCRIPTION: A threat actor named Akira Ransomware has reported possession of data from the Swedish municipality of Bjuv, which the group threatens to publish on the dark web. The data probably ended up in the group's possession in a series of data breaches in Sweden at the beginning of February. In this series, the main victim was Tietoevry, but the attack also exposed the systems of hundreds of smaller operators that used Tietoevry's services. However, there is no exact information on how Akira got hold of the data of the small municipality, nor is there any idea of what kind of data the group possesses outside the group's own claims.

ACTOR: Akira Ransomware.

MOTIVE: Unclear, Akira's modus operandi typically involves using ransomware and blackmailing data recovery. In this case, Akira doesn't even seem to demand a ransom, but simply threatens to leak the data.

EFFECTS: No exact information, as it is unclear what kind of data Akira may have in his possession. It may involve personal data, contracts and financial information of municipal residents, and their disclosure may lead to the realisation of many different threats, both to the municipality itself and to people living or companies operating there.

INFOSYS MCCAMISH SYSTEMS LLC AND BANK OF AMERICA -DATA-BREACH

DATE: Already 3.-24.11.2024, but the information was released in 1.2.2024

DESCRIPTION: Data belonging to about 57,000 customers of Bank of America ended up to threat actor as a result of a data breach involving the bank's partner. The leaked information may have included customers' names, physical and email addresses, dates of birth and social security numbers.

ACTOR: Lockbit

MOTIVE: Financial

IMPACT: The announcement of the incident this late has caused some confusion and dissent and it has been speculated to be a possible violation of the law. Whether that be the case, it has at least caused reputational damage to organisations. For the average customer, leaked information can expose one to an identity theft, for example. In return, Bank of America has offered its customers a free two-year service to for identity protect.



ACTIVE THREAT ACTORS

MOGILEVICH RANSOMWARE

DESCRIPTION: Criminal group first detected in February 2024. Declared itself to be a purely financially motivated operator. Advertises itself as a Ransomware-as-a-service (RaaS) actor, and actively seeks partners from other hacker groups.

RECENT ACTIVITY: Reported hitting several targets during February. The biggest targets have been game manufacturer Epic Games and the Irish Ministry of Defence. However, both parties have stated that no attack has taken place. In addition to these, none of the other targets of the group's self-reported attacks have publicly admitted to the attacks, and the group has not published evidence of successful attacks.

METHODS AND TACTICS: Unlike many other extortionists, they do not publish "samples" of the data they steal. This, combined with comparatively low ransom demands, has led many to believe that the group's self-reported attacks are false, and instead of actual blackmail, the group uses low ransom demands and threatening messages to pressure the victim into paying without any data even being hijacked.



LOCKBIT

DESCRIPTION: One of the best known and largest Ransomware as a Service (RaaS) actors. Sells the ransomware it develops to its subcontractors who carry out the actual ransomware attacks.

RECENT ACTIVITY: Suffered heavy losses during February due to an international police strike. The group's online services and the data servers running them ended up in the possession of the authorities, and with them a lot of data, including ransomware decryption keys. In addition to this, cryptocurrency accounts managed by the group were frozen. Despite the losses suffered by the group, the subcontractors carrying out ransomware attacks seem to be carrying out almost normal attacks, at least for the time being. In the coming months, it is good to monitor how this activity develops.

PROCEDURES AND TACTICS: This ransomware is used for precisely targeted attacks that prevent the target from accessing the computer system in exchange for a ransom.



CACTUS

DESCRIPTION: A hacktivist group that has been active since at least March 2023

RECENT ACTIVITY: In February, the group struck the data networks of AB Tesel, a Dutch agricultural and food production logistics company. 1TB of data has allegedly been hijacked. French Schneider Electric, a manufacturer of electrical equipment and components, also suffered a ransom attack by the group in February. In this case, 1.5TB of company data has allegedly been hijacked. As of March 2023, the group has added more than 100 companies or organizations to its data breach site.

METHODS AND TACTICS: The group leverages purchased credentials, partnerships with various malware actors, phishing attacks, and security vulnerabilities. Among other things, the group has exploited vulnerabilities in VPN programs.



COMMERCIAL SPYWARE COMPANIES: CY4GATE, RCS LABS, IPS INTELLIGENCE, VARISTON IT, TRUEL IT, PROTECT ELECTRONIC SYSTEMS, NEGG GROUP JA MOLLITIAM INDUSTRIES

DESCRIPTION: Meta, the giant behind Facebook and Instagram, released its threat report in February that looks at security events of the fourth quarter of 2023. As a new finding, the company detected eight new commercial spyware operators registered in Italy, Spain and the United Arab Emirates.

RECENT ACTIVITY: The companies have targeted iOS, Android and Windows devices in order to gain access to the device and thus the target's personal information.

METHODS AND TACTICS: In general, spyware is considered a significant threat not only to individuals, but also to society at large. Authoritarian states have used commercial spyware, for example, to spy on opposition politicians. Many spyware programs can be delivered using the so-called "zero click" method, which does not require the victim to make a security mistake or leave traces on the device. The companies in question have also stepped up their efforts by creating fake profiles on social media and by distributing an infected version of WhatsApp.



A PASSION
FOR A SAFE
CYBER WORLD



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.



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



OUR SERVICES



Management Advisory Services

We are experienced and trusted experts and management advisors. We give support in comprehensive security, cybersecurity, internal security, and third party risk management. Our working methods include, for example, theme presentations, background memorandums, workshops, and scenario work.

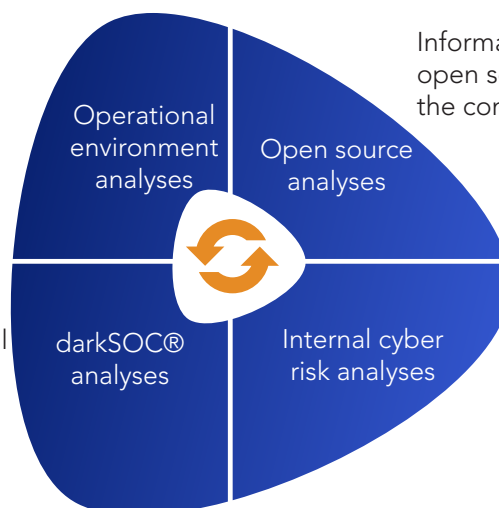


A Comprehensive Situational Picture

A comprehensive situational picture of cybersecurity is created with the help of the modular service developed by Cyberwatch Finland, for which the necessary data is collected using numerous different methods.

By analysing the operational environment from different perspectives, an overall insight is formed about the events, phenomena, and trends affecting the organisation.

The dark and deep web data is collected non-stop at 9 Gb per second, from servers located all around the world.



Information collected from open sources complements the comprehensive picture.

With the help of internal cyber risk analysis, a comprehensive picture of the organisation's insider threats, and other risk factors are formed.

OUR SERVICES

Reviews

Cyberwatch's analysis team constantly monitors the cybersecurity operational environment by collecting and analyzing 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 and are declarative in nature.

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 and quarterly 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.

Monthly Review

The monthly review sums up, expands, and puts into context the themes and phenomena discussed in the weekly reviews.

The monthly review describes the development of phenomena, focusing on different perspectives of hybrid influencing.

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.

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.

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.

OUR SERVICES

darkSOC® – the Dark and Deep Web Analysis

With darkSOC® -analysis, we examine and report your organisation's profile and level of exposure in the dark and deep web. Data is collected non-stop at 9 Gb per second, from servers located all around the world. The analysis reveals organisation's cybersecurity deficiencies, data breaches, and other potential vulnerabilities. With the help of analysis, you get an overview of what the organisation looks like from the cybercriminal's perspective.

We prepare a written report from the analysis, in which we highlight key findings to support management's decision-making. The report also includes a more detailed presentation of the findings. We also give recommendations on immediate corrective actions and strategic-level development targets.



The Benefits of darkSOC®



Increases cyber intelligence capabilities



Anticipates constantly changing cyberworld



Complements company's cybermaturity



Serves as a forensic investigation tool



Supports organisational strategic decision-making



Complements strategic cyber situational picture



Discovers vulnerabilities and weaknesses



Facilitates cyber strategy process

OUR SERVICES

Analysis



The Surface Web Analysis

We form an external view of your level of cybersecurity in the surface network and compare your position with other organisations in the same industry. Our analysis is based on the platform of our global partner SecurityScorecard, whose data is based on a trusted, transparent classification method and data collected from millions of organisations. Based on our analysis, we make recommendations on corrective measures and draft a road map for their practical implementation in your organisation.

Powered by



The Open Source Analysis

We produce analyzes based on open sources on the topics you choose. We use advanced digital tools with which we search for information from public free and commercial sources as well as from various media and social media platforms. We refine the data into a form relevant to the goals of the analysis.



Internal Cyber Risk Analysis

With the help of an internal cyber risk analysis, it is possible to form an overall picture of insider threats and other risk factors related to your organisation's cybersecurity.

We analyse the up-to-dateness and comprehensiveness of your organisation's cybersecurity policies, guidelines, instructions and other documentation. In addition, we interview the selected management members and other key personnel.

As a result of the analysis, you will have an image of the balance between your organisation's operation and the internal guidelines and external regulations that guide it, as well as a road map for developing the operation.



OUR SERVICES

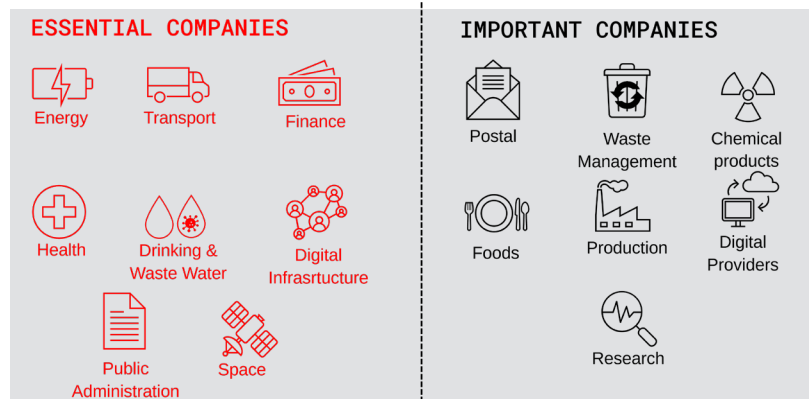
Analysis

NIS2 Gap analysis

The aim of the NIS2 Cybersecurity Directive is to improve the basic level of cybersecurity in the EU and to ensure the continuity of operations of critical entities

The directive entered into force on 17.1.2023, with member states having time to put things in order by 17.10.2024.

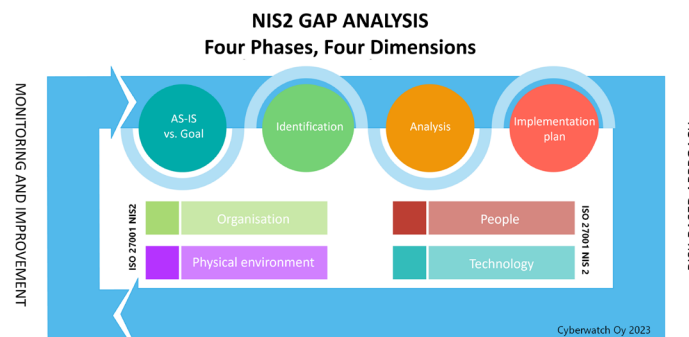
NIS2 cyber security directive concerns the following fields:



The minimum requirements of the NIS2 Cybersecurity Directive are:

1. Policies on risk analysis and information system security
2. Incident management
3. Business continuity, such as backup management and recovery, and crisis management
4. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
5. Security in network and information systems acquisition, development and maintenance, including vulnerability management and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
7. Basic cyber hygiene practices and cybersecurity training
8. Policies and procedures regarding the use of cryptography, and appropriate encryption means
9. Human resources security, access control policies and asset management
10. The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Preparing the equivalency of current state of your organisation with the minimum requirements should be started well in advance. Cyberwatch's NIS2 gap analysis is a risk-based approach to the minimum requirements, using not only the directive but also the ISO 27001 standard and related management measures as a framework. With the help of the analysis, the organisation can direct development activities to the right targets.



OUR SERVICES

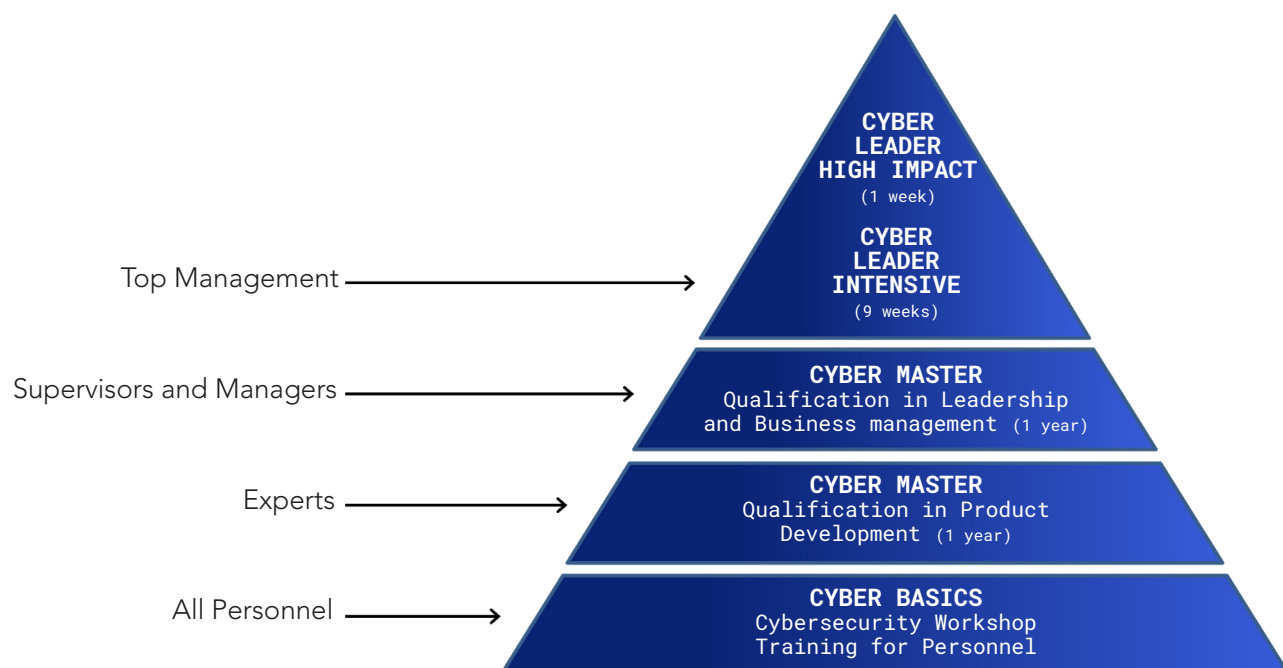
Training and Competency Development

We produce training for the Cyber Master specialist vocational qualification in co-operation with the Management Institute of Finland MIF Oy.

Currently, in the programs, it is possible to complete the Cyber Master qualification in leadership and business management as well as in product development.

We also provide tailored training for your organisation, which helps to strengthen your organisation's cybersecurity skills and helps you to be better prepared for the challenges of the digital operating environment.

Our all training offering consists of modules, from which student or organisation can choose the options according to their needs.



OUR SERVICES

Forensic services

Investigations and Special audits

We support organisations in all cases of misconduct related to their activities in investigating suspicions and violations. We have extensive experience in corporate investigations and special audits.

Our expert experience consists of, among other things, numerous frauds and corruption schemes as well as different types of violations of the code of conduct.

Background checks

We review the reputation, integrity and operating history of companies and related individuals by collecting and analysing information to support our client's decision-making in various situations, such as M&A situations or dealing with third parties such as contractors and service providers.

Risk Management Services

We help your organisation to identify, assess and manage risks that may affect your operations.

In addition to our experienced subject matter experts we utilize modern risk management technologies.

Anti-Money Laundering (AML)

We support your organisation in fulfilling the obligations of the Anti-Money Laundering Regulation.

Know Your Customer (KYC)
Customer Due Diligence (CDD)

Supporting in prevention of money laundering and terrorist financing:
policies, programs, risk assessments.



Cyberwatch eWHISTLE Channel

Cyberwatch eWHISTLE whistleblowing channel is a responsible, secure, and privacy-secured whistleblowing channel with a clear environment for processing, investigating, and making decisions. The legislation compliant eWHISTLE offers ready-to-go packages, or a service tailored to your needs

We plan and implement the whistleblowing channel from the beginning to the very end. Our experts help you create a compliant report management and investigation process and the required documentation related to the whistleblowing channel. After the implementation of the service, we receive reports, assess them, and propose further actions to you. If requested, we support you in investigating the incident.

The technical platform of the eWHISTLE is produced Easywhistle Oy. The system is easy to access, data secure and user friendly. The service is available in all needed languages. The channel fulfils the GDPR-requirements, and the servers are located in the EU.





A PASSION FOR A SAFE CYBER WORLD



Contact

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
ake@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi

FOR A BETTER DIGITAL FUTURE

Technology and digitalisation are changing people's behaviour, business practices, and market dynamics. Cyber Security Nordic will explore cybersecurity from the perspectives of both businesses and public administration. The speeches will cover topics such as the impact of digitalisation on democracy and technology regulations, the increasing diversity of cyber-attacks, and approaches to risk management for critical functions of companies and societies.

Explore more at cybersecuritynordic.com



29–30 October 2024
Helsinki Expo and Convention Centre

MESSUKESKUS
The real social media