

Special media of strategic cyber security

# Cyberwatch Finland

MAGAZINE 3 / 2023

## SMART CYBERSECURITY

ARTIFICIAL  
INTELLIGENCE  
AND CRIMINALITY

FOUR SCENARIOS  
FOR THE USE OF  
CYBER WEAPONS  
& DETERRENCE

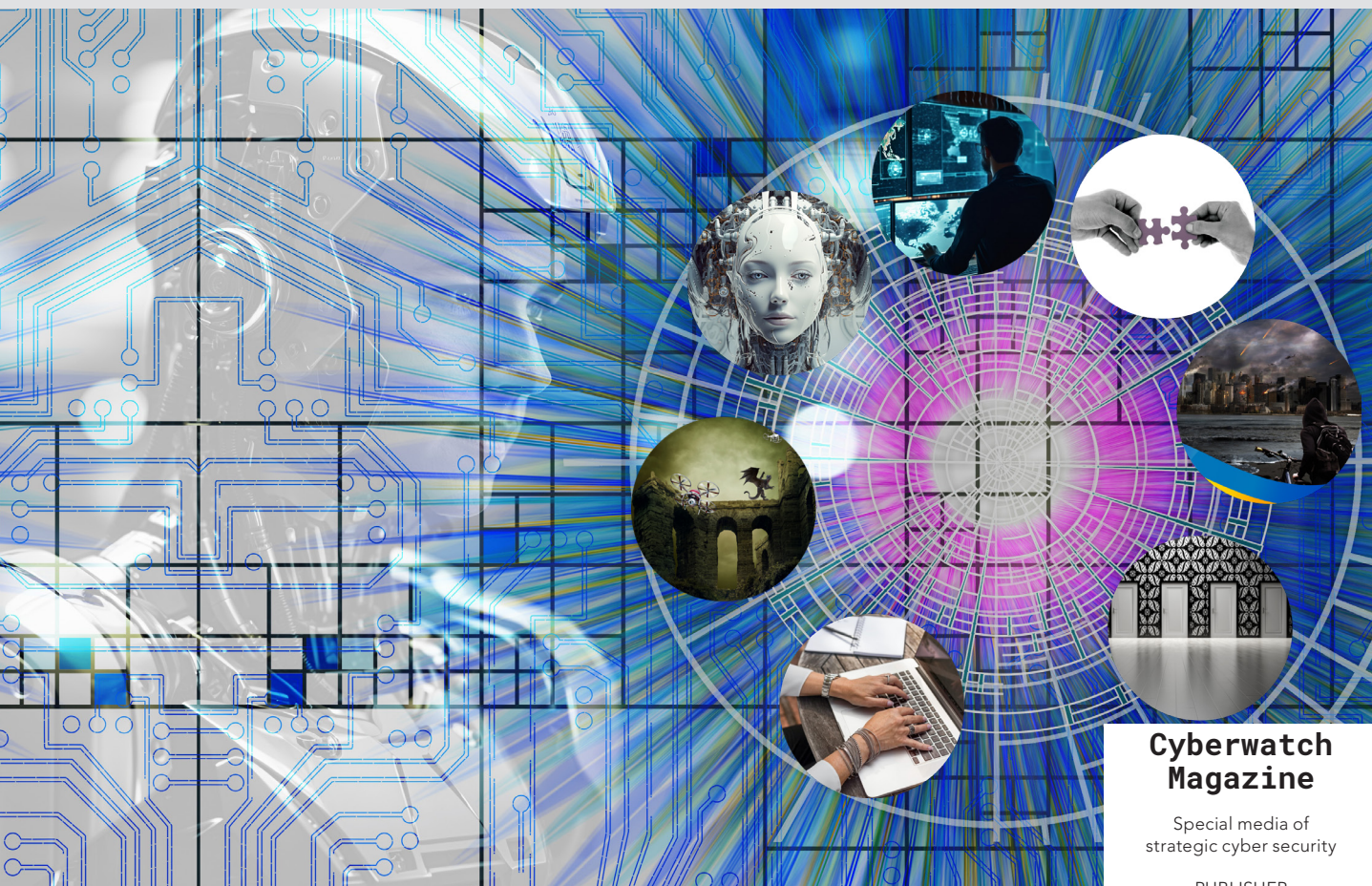


Cybersecurity is built by small actions and management of large concepts



# CONTENT

3/2023



**3**

There is a Need for Smart Cybersecurity!

**4**

Four Scenarios for the Use of Cyber Weapons & Deterrence

**10**

Finnish Cybersecurity Industry Offers Solutions for the EU's Digital Agenda

**12**

Every Second Matters- Preparedness and Crisis Communication as a Critical Part of Cybersecurity

**15**

Artificial Intelligence and Criminality

**18**

Game of Drones: The Increasing Role of Drones in Modern Warfare and the Ukrainian War

**29**

The Cyber Competence of the Company's Personnel Develops Through Cyber Master Courses

**33**

The War in Ukraine is Also a Question of Information- and Cyber Dominance

**40**

Monthly Review October

**51**

Threat Intelligence Review

**54**

Samples from Cyberwatch Finland Weekly Reviews

## Cyberwatch Magazine

Special media of strategic cyber security

PUBLISHER  
Cyberwatch Finland  
Nuijamiestentie 5 C  
04400 Helsinki  
[www.cyberwatchfinland.fi](http://www.cyberwatchfinland.fi)

THE EDITORIAL TEAM  
Editor-in-Chief  
Aapo Cederberg  
[aapo@cyberwatchfinland.fi](mailto:aapo@cyberwatchfinland.fi)

Subeditor  
Elina Turunen  
[elina@cyberwatchfinland.fi](mailto:elina@cyberwatchfinland.fi)

LAYOUT  
Elina Turunen  
[elina@cyberwatchfinland.fi](mailto:elina@cyberwatchfinland.fi)

ILLUSTRATIONS  
Unsplash  
Pixabay  
Shutterstock

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

PRINT HOUSE  
Scanseri Oy, Finland

# THERE IS A NEED FOR SMART CYBERSECURITY!

// Aapo Cederberg

The global security situation is increasingly unstable and worrying. Surprises and unpredictable crises arise all the time. It feels like no one is safe from the ripple effects of crises. In modern societies, digitalisation is linked to all aspects of life and, above all, to the functionality of vital services and critical infrastructure. That's why the number of cyberattacks on the critical targets has doubled over the past year. The selection of targets is more careful and based on effective intelligence and vulnerability scanning. Intelligence information is exchanged on the dark web between state actors and cybercriminals. It is becoming increasingly difficult to know who is really behind the attacks. Technical attribution is difficult and slow. The importance of political attribution should be emphasised: hybrid and cyber operations are increasingly linked to political goals and influencing operations.

Cybersecurity arrangements in different organisations mainly follow the same principles and solutions. The question arises, is the current level enough? The "crown jewels" of cybersecurity are threat intelligence, preventive measures and crisis resilience. With effective cybersecurity one also achieves deterrence. Therefore, there is a high demand for developing offensive cyber capabilities. Great powers are developing their counterstrike capability, and cybercriminals are developing their concepts and criminal services. Globally, cyberattacks cause losses of six trillion dollars annually. It is therefore a question of destiny for our entire global well-being.

Future well-being requires more agile and intelligent cybersecurity services and technologies. Technological solutions can be developed efficiently with the help of artificial intelligence. However, the fight against cyberattacks emphasises the role of people and human factors. Therefore, the protection and prevention of attacks requires better intelligence and defensive capabilities. The importance of dark and deep web analyses is emphasised in anticipating the plans and intentions of criminals and state actors. Even this alone is not enough: the analyses of the obtained data and capacity to draw right conclusions are key to success. We must be one step ahead of the attackers.

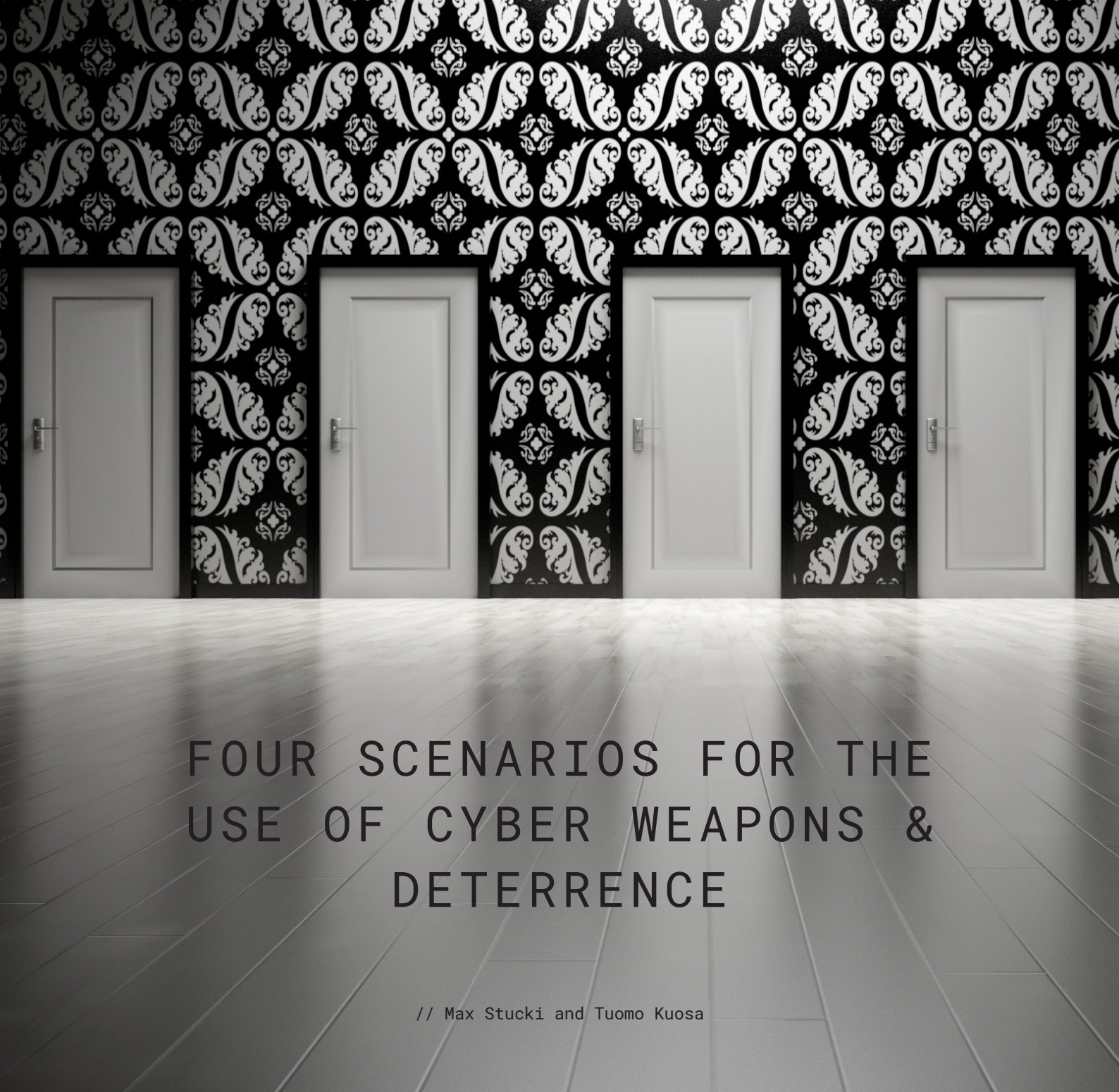
The EU Cybersecurity Directive (NIS2), which entered into force at the turn of the year, requires critical actors in society to take "appropriate and proportionate technical, operational and organisational measures". This too, highlights the urgent need to develop smarter and more cost-effective solutions and measures. Now is exactly the right time to invest in smart cybersecurity and innovation of the new solutions. Let's do it together. ■



**AAPO CEDERBERG**

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





# FOUR SCENARIOS FOR THE USE OF CYBER WEAPONS & DETERRENCE

// Max Stucki and Tuomo Kuosa

Cyberweapons are malware, such as viruses or spyware, used to harm adversary's critical infrastructure. Cyberweapons may constitute cyber deterrence, a set of offensive cyber capabilities that create a threat of retaliation dissuading potential attackers, and defensive capabilities that make cyberattacks less appealing. In the future, we may witness a massive cyber arms race that creates a fragile balance of terror between the great powers. We may also see large scale cyberwarfare. On the other hand, it is also possible that either progress in cybersecurity or lacking investment in cyberweapons make the cyber operations less appealing than anticipated.



## BACKGROUND

A cyberweapon is basically a malware such as a virus, trojan, worm, spyware or other corrupting computer code that can be used in cyberattacks. They cause harm in the adversary's computer networks and systems, subvert or cause harm to digital structures, or try to obtain valuable data or reach some other, often political or military, goal. Such weapons are designed to achieve objectives that otherwise would require using military force, sabotage or espionage.

Cyberweapon can be understood as the same as hacking, but it may be more accurate to see it as a set of different types of malwares, including private hacktivist groups' actions, that state actors can use simultaneously to make a larger scale attack on other countries than with a single malware. The exploitation, destruction, or degradation of the opponent's information assets can be considered some of the main aims of cyberweapon use. Perhaps the best-known cyberweapon example to date is the Stuxnet malware that was used to sabotage the Iranian nuclear program.

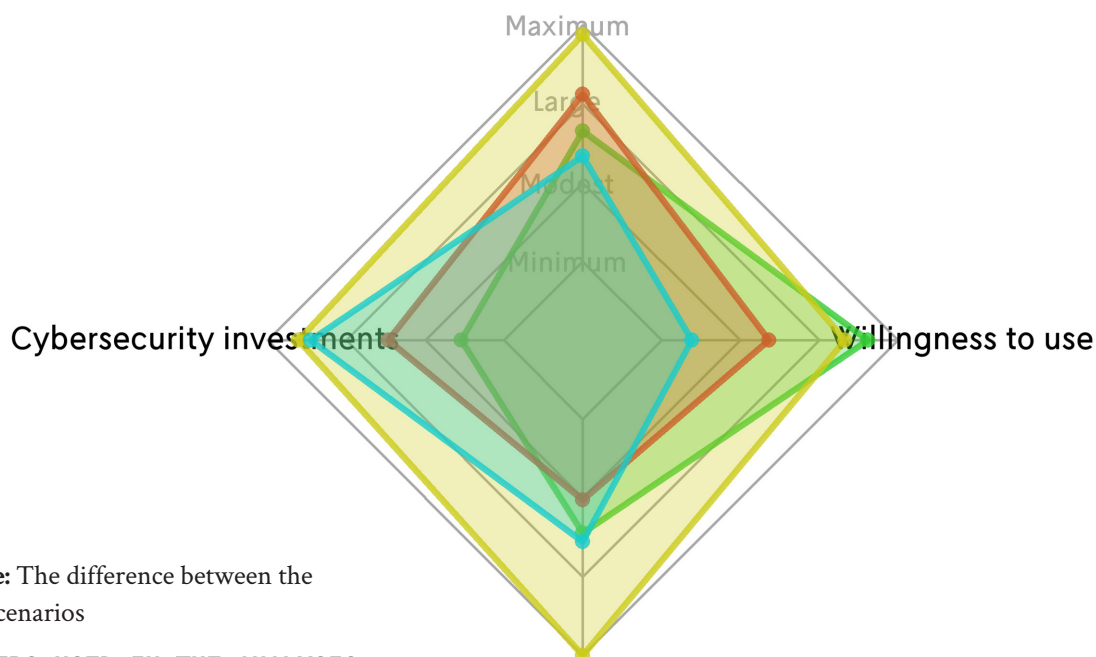
Cyber deterrence refers to the offensive cyber capabilities an actor has that by their existence create a threat that

dissuades potential aggressors from pursuing their aims via cyber means. However, cyber deterrence has been criticised as a problematic concept that cannot be compared, e.g., to the traditional nuclear deterrence, as it is basically just about the threat of cyber revenge where it is even unclear who is the attacker. Hence attribution problems and credibility of digital capabilities, including cyber deterrence by denial, i.e., increasing cybersecurity and system resilience making cyberattacks less appealing, are but few of the issues that need to be resolved before cyber deterrence reaches maturity.

At the start of Russia's invasion of Ukraine in 2022, President Biden was allegedly presented with an option to strike at Russia's internet connectivity, electric power, railroads and other software that are crucial for the state to function by using cyberweapons that the US is known to have been developing for years. However, the US decided not to make such an attack. The possible reason for this is that it wanted to keep the deterrence in stock instead of using the full arsenal at this point, as cyberweapons can usually be used just once because the opponent knows where their weak spots are after the usage and prepares accordingly.

## FOUR SKENARIOS

Main actors: USA, China, Russia, Israel, UK, hacker groups.



**Image:** The difference between the four scenarios

### DRIVERS USED IN THE ANALYSIS:

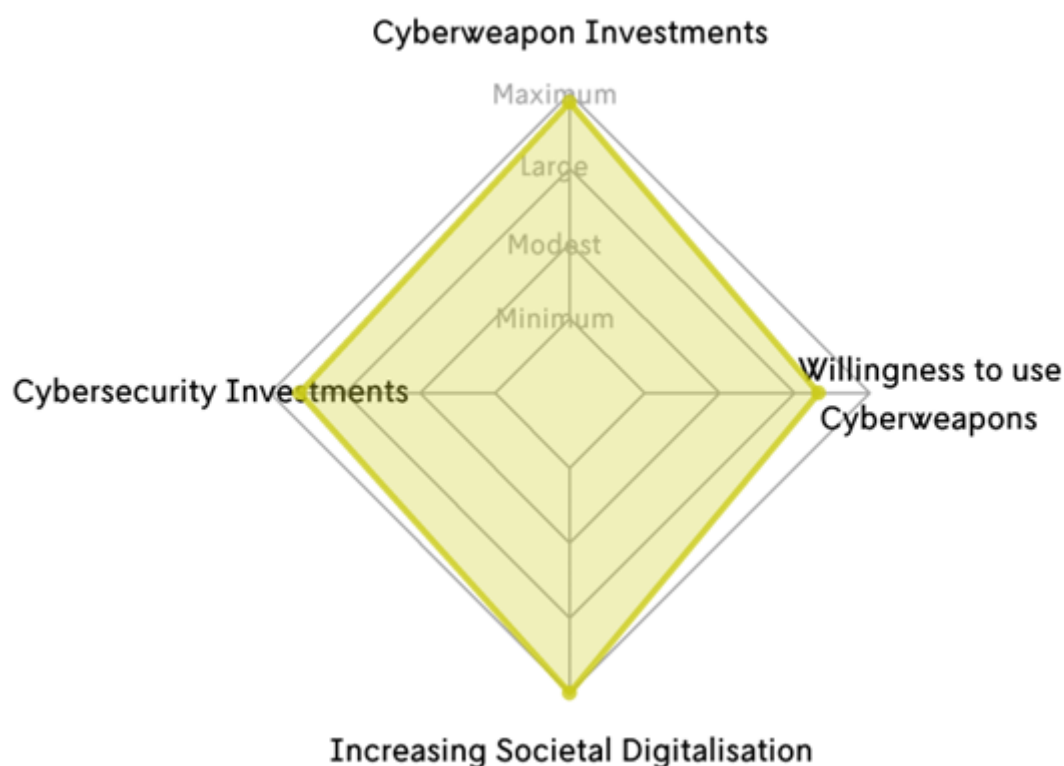
- Cyberweapon investments
- Willingness to use cyberweapons
- Increasing societal digitalisation
- Cybersecurity investments





## SCENARIO 1: CYBERWEAPONS ARMS RACE

The increasing reliance on digital services has made cyberweapons a significant tool in international power politics, prompting investments in cybersecurity as well. The world is in a cyber arms race, with economic blocs sharing cyberweapons and preparing for a potential massive cyber strike.



**Image:** the role of each driver of uncertainty in this scenario.

Cyberweapons are becoming a significant tool in international power politics. As societies have become fully reliant on digital services, striking opponent's vital systems is now a tempting option for causing damage. Massive investments in cyber capabilities are also boosting investments in cybersecurity. Although cyber means are being used below the threshold of actual war, a fragile balance of "mutually assured cyber destruction" is developing between the great powers. Most countries are willing to use some cyber means, but an all-out cyber-attack aimed at taking down most of the control systems in a country has not been witnessed yet. The world, and especially the economic blocs that are sharing the cyberweapons, are locked in a cyber arms race as everybody is preparing for the massive cyber strike that hopefully never materialises.

### DEVELOPMENT PATH FOR SCENARIO 1:

**2025:** Digital infrastructure everywhere is now a high-priority target for cyber operations. More potent and capable cyber means are developed to harm adversaries and retaliate when an attack is carried out.

**2027:** Investments in cybersecurity start to soar as both public and private organisations are more and more subject to attacks presumably perpetrated by hostile states via criminal hacker groups.

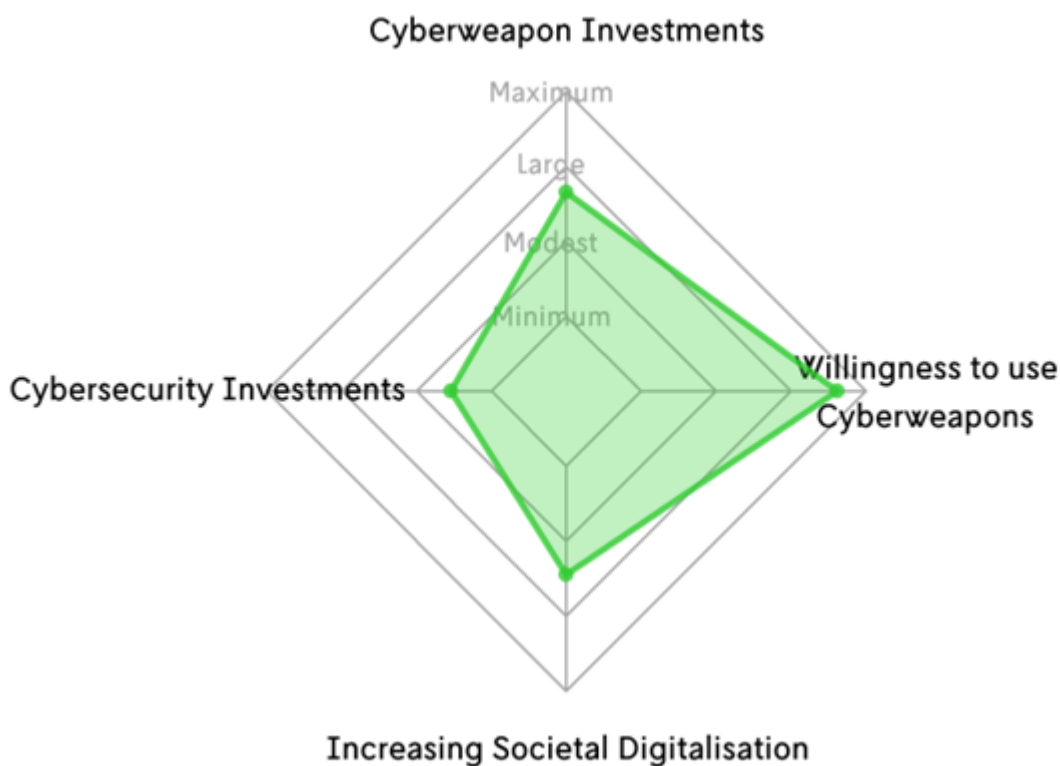
**2028:** The cost of developing capable cyberweapons is increasing as the security systems become increasingly sophisticated and capable.

**2030:** The United States announces it can take out China's vital systems without any kinetic operations. China claims that it could retaliate in kind. Russia announces that a sufficiently extensive cyber-attack that harms its vital systems will be retaliated with nuclear weapons.



## SCENARIO 2: WEAK CYBERSECURITY LEADS TO INCREASED USE OF CYBERWEAPONS

Despite some advancements in cyberweapons and cybersecurity, they do not live up to their expected potential in inter-state warfare. However, due to weak cybersecurity, cyberweapons remain an attractive option for criminal and terrorist groups.



**Image:** the role of each driver of uncertainty in this scenario.

Both offensive cyberweapons and cybersecurity see some development, but cyber capabilities do not become a game changer in inter-state warfare as was anticipated. In part this is because of the increasing willingness of many states to ensure that they can also operate if their digital systems are taken out, or they refuse to connect them to the internet altogether – thus making the list of targets smaller and less appealing. However, limited cybersecurity capabilities make cyber-attacks tempting to criminal and terrorist groups who can cause some damage with them, especially in the private sector. Cyberweapons cannot be used to build up a real deterrence against a foreign attack. Rather, they are another tool for politicians, but real firepower is still needed to cause significant damage.

### DEVELOPMENT PATH FOR SCENARIO 2:

**2025:** Cyberattacks are getting more common in a world with growing power politics and where the concealment and deniability is getting easier.

**2028:** Cyberattacks are increasing in power and duration. Cybersecurity is not keeping up with the development. The economic costs are immense.

**2030:** States are increasing spending on critical offline infrastructure and using unconventional alternative systems next to digital ones.

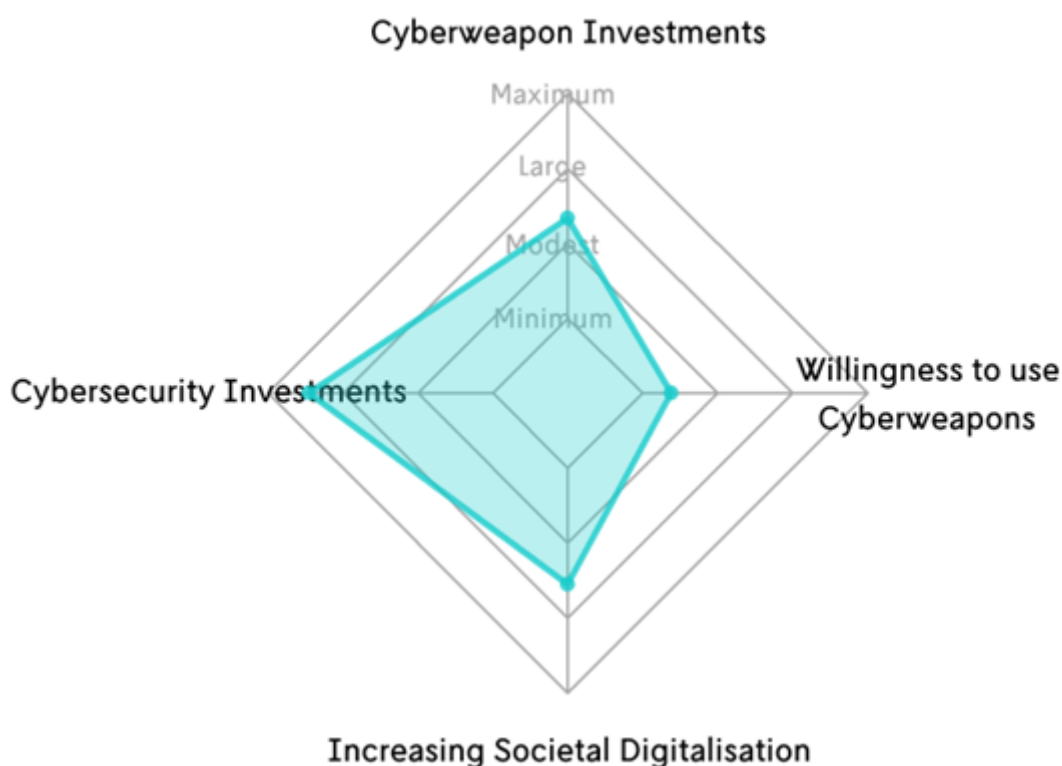
**2035:** States build alternative, slower but more robust secondary systems that are used in cases of cyber-attacks. Governments uphold some specific cyberweapon capabilities, but investment in them remains low.





### SCENARIO 3: HEAVY INVESTMENTS IN CYBERSECURITY DETER THE USE OF CYBERWEAPONS

Cybersecurity investments in both public and private sectors are increasing, leading to fortified systems that deter malicious actors and decrease the appeal of cyberweapons. Cyber resilience is becoming more important, with systems designed to withstand attacks and quickly return to normal functioning. Although the cyber domain is very significant, critical vulnerabilities are low.



**Image:** the role of each driver of uncertainty in this scenario.

Both public and private sectors are investing heavily in cybersecurity. Vital systems that keep both society and businesses running are being fortified against malicious actors. High cybersecurity investments seem to make the use of cyberweapons less efficient and appealing, decreasing the investments states are willing to make to acquire them. Cybersecurity is increasingly based on cyber resilience – even though all attacks cannot be deterred, the systems themselves can withstand assaults and shocks and return to normal functioning quickly. The cyber domain remains important, but it does not contain significant numbers of critical vulnerabilities anymore.

#### DEVELOPMENT PATH FOR SCENARIO 3:

**2025:** Cyberweapons are used often and are becoming a real nuisance for governments.

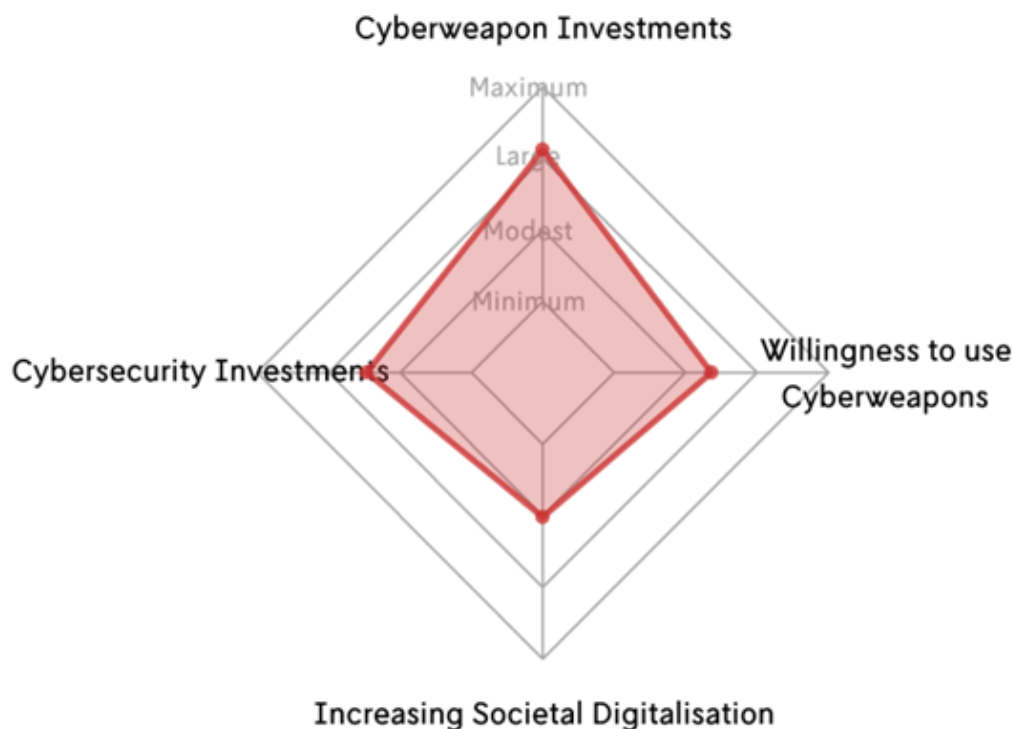
**2028:** There is a breakthrough in AI, and together with blockchain they greatly increase cybersecurity and its applications.

**2030:** It has become much more costly to break a system than what is to be gained by it. Expenses related to high offensive cyber capabilities make efficient cyberattacks too costly for other actors than states.

**2035:** Cyberweapons have become nearly useless against developed states.

## SCENARIO 4: CYBERWEAPONS DEVELOP MODERATELY

Investment and development in offensive and defensive cyber capabilities continue; however, the hype surrounding the cyber domain levels off. Despite the normalisation of cyberweapons as part of the arsenal of major international actors, there is still no clear concept of cyber deterrence, and the threat of cyber-attacks remains less tangible.



**Image:** the role of each driver of uncertainty in this scenario.

Cyber capabilities, both offensive and defensive, see further investment and development. However, the buzz around the cyber domain has plateaued. Cyberweapons and cybersecurity are issues among other security matters that the states and businesses face. In many ways, cyberweapons have been normalised and they are part of the arsenal of any significant actor in the international arena. Yet, there is no clear concept of cyber deterrence – the problems related to attribution, capability demonstrations and other matters make the threat of cyber-attacks less tangible. Nobody really wants to show their hand when it comes to cyberweapons, lest the opponent notice the bluff, i.e., that “the emperor has no clothes”.

### DEVELOPMENT PATH FOR SCENARIO 4:

**2025:** Cyberweapons have become an established and important part of the arsenal of most militaries. However, large-scale deployment of cyberweapons aiming to seriously harm other state’s critical systems has not been witnessed yet.

**2030:** Cyberweapon capacities are widely proliferated. This increases demand and investments on cybersecurity. Economic blocs do a lot of cooperation in cybersecurity.

**2035:** Although all developed states claim to possess significant cyber capabilities, it still remains somewhat unclear whether they can ever compete with traditional kinetic means when it comes to causing harm to critical infrastructure. ■



**TUOMO KUOSA**

- Dr. Tuomo Kuosa is a co-founder, and the Director of Futures Research Team in Futures Platform.
- Futures Platform**



**MAX STUCKI**

- Max Stucki has worked as a strategic foresight consultant and analyst for several years. He has helped numerous public and private organisations in their efforts to study and make sense of the future.
- Futures Platform**







# FINNISH CYBERSECURITY INDUSTRY OFFERS SOLUTIONS FOR THE EU'S DIGITAL AGENDA

// Peter Sund and Risto Rajala

Cybersecurity is ever more topical matter in a world that is going through rapid digitalization. Our critical infrastructure, such as logistics, electricity grids and water management, as well as most other services depend on connected information systems. At the same time, many of us own and use several connected devices constantly in our daily lives, trusting them with both our everyday affairs and most sensitive and important personal data.

Thankfully, our legislators are paying a lot of attention to the security of the digital domain. During the ongoing election cycle, the European Union (EU) has followed an ambitious agenda to build better digital life for Europeans, with increased level of cybersecurity as one of its corner stones. The EU is currently processing, and has already adopted, landmark regulatory initiatives that will significantly improve cybersecurity in all Europe. NIS2 directive, adopted in late 2022, will lay out renewed rules and responsibilities for companies and other entities that are deemed critical for functions of European societies. Proposal for Cyber Resilience Act has entered trilogues phase, where European Commission, member states and European parliament are ironing out its final details. Once adopted, Cyber Resilience Act will introduce horizontal cybersecurity rules for all connected devices and software. Together, these two initiatives will make our daily lives more secure and raise the bar for cybersecurity measures to a level suitable for our connected societies.

Despite all the good efforts that are currently going on in the EU, there are also legislative proposals that are at best counterproductive and at worst threatening to derail the entire digital agenda, as well as cybersecurity in Europe. Proposal for Cyber Solidarity Act has an important objective to enhance detection, analysis, and response to cyber incidents, as well as information-sharing in

member states. Unfortunately, the legislative proposal has been prepared in haste and without appropriate impact assessments. Proposed measures appear to be ineffective, depriving scarce resources from other needs, as well as judicially dubious. There is also a real risk for market distortions. Hopefully the proposal will be amended by the co-legislators and its impacts properly scrutinized. Simultaneously with Cyber Solidarity Act, the Commission published a communication for Cyber Skills Academy, which would basically be an online platform to serve a single point of entry for cybersecurity training offers, certifications, funding opportunities and any other existing initiatives aimed at promoting cybersecurity skills. While intentions behind Cyber Skills Academy are sensible, the actual benefits of setting up such a platform remain unclear. To truly tackle the cybersecurity skills shortage, the current solutions for arranging cybersecurity education need to be reformed, enhanced, and scaled up. And this is the task of the member states. At the same time, it is important that unnecessary bureaucratic structures that would exclude many of the educational institutions (i.e. trust labels) are not created.

Even more problematic is the proposal to weaken end-to-end encryption (E2EE) in electronic communications services, to enable authorities to scan private communications. If accepted, the proposal would create an unprecedented surveillance apparatus that violates fundamental rights. Such an idea is connected to the objective of better prevent and combat Child Sexual Abuse (CSA) which every sensible person obviously supports, but the proposed way to achieve this important objective would be deeply problematic. Legal and constitutional concerns regarding the proposal have been raised in many contexts and the proposal is also in conflict with Cyber Resilience Act proposal. Encryption plays a crucial

role in providing private and secure communications that users, including children, demand and expect to keep them safe online. Even well-intentioned efforts to provide a lawful intercept solution in end-to-end encryption will undermine critical security benefits by making all users of such services more vulnerable to malicious attacks. Creating any kind of backdoors or limitations of confidentiality to electronic communications services for authorities would unavoidably mean that the same backdoors could be used for other government purposes that would significantly undermine digital trust and would be available for criminals as well. They would most certainly try to find those.

The ones with most to lose from the weakening of end-to-end encryption are ordinary Europeans and businesses, whose privacy would be invaded and who would lose access to secure communications services. Criminals and other malicious actors, however, would most likely find other ways to communicate in secret. It is essential that those member states who support weakening end-to-end encryption, such as Spain, Hungary, and Cyprus, as well as those who have remained ambiguous, reconsider their positions according to the vital concerns regarding European's fundamental rights and maintaining digital security. A clear position should be included to the final Regulation not to require any weakening to end-to-end encryption technology. Commendably, Finland is among those member states, such as Estonia, Germany and Austria who have been able to see also the negative consequences of the idea in protecting fundamental values. The Finnish Parliament just declared their position by requiring that authorities' coercive powers do not in fact lead to the general weakening or dismantling of end-to-end encryption or other similar security measures, or to the restriction of their use, and thereby to the deterioration of the level of security and cyber security of communication and related services.

Once completed, hopefully in a manner that is consistent with fundamental rights and digital security that are existential for individuals and businesses alike European cybersecurity agenda will enter to the implementation phase, which crucial in ensuring that adopted regulations serve their purposes and reflect the political decisions behind them. It is essential that member states start accreditation process for entities capable to perform third party assessments to products and software that are deemed critical in Cyber resilience act well in advance. Successful and concordant implementation of regulations has the potential to provide immense economic benefits, of course among those that come with better digital security, while failure might seriously hinder competitiveness of European industries. At the same time, genuine public-private partnerships are needed all over Europe to ensure that the level of cybersecurity is increased throughout societies and especially in the private sector where the ownership for majority of information systems and critical infrastructure actually is.

Even with appropriate regulations in place, increased level of cybersecurity will not be achieved without state-of-the-art products, services, and solutions. This calls for major EU-level efforts to support development and deployment of new cybersecurity technologies. Fortunately, Finnish cybersecurity industry has a lot to offer for implementation of new EU regulations and has the capability to offer its expertise all over Europe and beyond. Finnish cybersecurity industry consists of companies with various portfolios, from world class technologies to human-centric applications to empower people to take care of their own digital security. ■



**PETER SUND**

- ’ CEO
- ’ Finnish Information Security Cluster (FISC)

**Technology Industries of Finland**



**RISTO RAJALA**

- ’ Advisor
- ’ Finnish Information Security Cluster (FISC)

**Technology Industries of Finland**





# EVERY SECOND MATTERS- PREPAREDNESS AND CRISIS COMMUNICATION AS A CRITICAL PART OF CYBERSECURITY

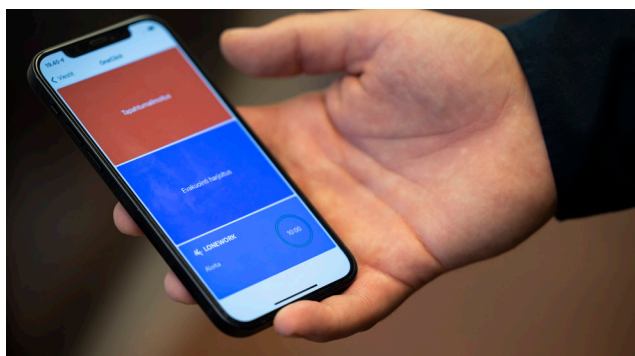
// Kari Aho

The recently tightened international situation has made it clear that we live in an increasingly uncertain and threatening world. Cyberattacks, system failures, power outages, and physical security threats are just a few examples of scenarios that can cause significant harm to individuals and organisations. The situation is further complicated by the fact that different crises can overlap and affect each other. As these threats grow and become more complex, every second lost can be costly – not only financially, but also in terms of human lives and societal stability. Tightening regulation or the requirements set by the operating environment also create pressure to establish the necessary measures. In this constantly changing environment, preparedness and timely communication are especially emphasised.





According to a study published in 2021 by the international research company Gartner, an IT system failure alone causes an average cost of more than 5,300 euros per minute of failure. When you calculate what it means in just one hour, the amount rises to a staggering 318,000 euros. Such costs can arise, for example, from production line stoppages in industry, malfunctions of vital equipment in healthcare, or in larger organisations from a situation where commonly used communication systems, such as email or instant messaging solutions, are not available. This prevents employees from performing their tasks at least partially and can lead to significant production losses. The above is complemented by the IBM 2023 study, according to which the average cost related to data breaches is 4.25 million euros, which is a 15% increase compared to the situation three years ago.



I am Secapp Oy's CEO, Doctor of Information Technology, Kari Aho, and I will introduce a few main points regarding cyber and hybrid threat preparedness and the basics of crisis communication. At Secapp, we have been working with the private sector, authorities, and public administration for more than ten years on issues related to preparedness, critical communication, and alerting, and we produce related SaaS services. Last year, more than 10 million alerts were sent with Secapp related to various emergency situations.

When we discuss about cybersecurity and possible cyberattacks, our thoughts often turn to technical solutions and protection mechanisms, which are of course an important part of the whole. However, people's preparedness and readiness for action play at least an equally important role: how an individual person, organisation, and the necessary stakeholders act when a crisis occurs. What general operating instructions are related to the situation? How do you reach people and ensure reachability regardless of the time of day? What backup arrangements are followed when normal operating methods or systems are not available? Who takes the lead and directs the action? Who is responsible for communicating the situation to other stakeholders or the public? When and how is information collected and updated? And who decides the measures to be taken and that the emergency is over and normal operations can be returned to?



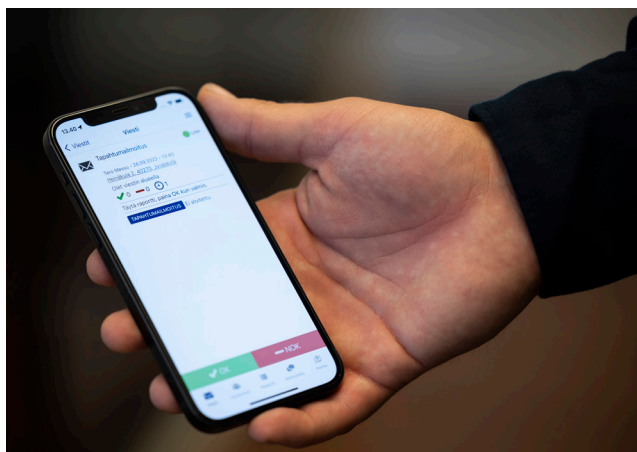


However, the unfortunate fact is that still 51% of organisations plan to increase investments in preparedness, training, and necessary tools only after a threat has once materialised. Here is a short checklist of five points, what kind of things, in addition to technical tools and protection mechanisms, should be considered as part of preparation:

**1** In crisis and disruption situations, human errors and forgetfulness easily occur, so plan necessary instructions and, for example, messaging groups for different situations in advance. In this way, you ensure that all essential persons receive the correct information in a timely manner in a crisis and know how to act as situation requires.

**2** Ensure that people are reachable, and that shared information is up to date, regardless of the communication device or technology they use. Some still have the old Nokia while others have the latest smart device. You don't necessarily have in the home sofa the emergency phone with you either, even if it's important to be available all the time. Also, in the event of a breakdown, you cannot always rely on all technologies working, so please consider possible backup numbers or contact methods beforehand. Also, without forgetting the safe processing of contact information so that it does not become available to third parties.

**3** The content of the communication can be very sensitive, and its falling into the wrong hands can itself cause, for example, dangerous situations or damage to reputation. Ensuring the flow of information, creating a situational picture, and documenting the situation are, however, of paramount importance to resolve the situation. So, make sure where your data is located that only the relevant people can access to it. If management is not centralised or automated, then an ex-employee can easily get involved, or conversely, someone essential to the operation can be left out.



**4** Every second counts in crisis situations. Technology should not take those precious seconds, but things must happen in the simplest automated way or at least with the push of a button. Therefore, investigate the possibilities, which processes or methods of operation could be automated or speeded up, so that key personnel have time to focus on solving the situation in a crisis, instead of being on the phone, for example.

**5** Repeatedly remind of the agreed guidelines, practice, and encourage people to give development ideas to improve crisis management. In this way, the operating models remain fresh in the memory and are constantly being taken in a more advanced direction.

Although technology is a key part of preparedness, people's actions, communication, and cooperation are at least as important. Organisations must understand both the technical and human perspectives and must be trained and equipped with the right tools and protocols to operate efficiently and securely. From the point of view of tools, Secapp is an example of a modern solution that helps to develop preparedness and brings effective tools for fast multi-channel reaching of people. One of our customers has said that Secapp reduces the time needed to reach people by up to 90%. I can say that I am proud of how Secapp helps make the world a safer place. Every second matters. ■



**KARI AHO**

- › CEO and co-founder
- › Secapp is helping organizations to manage crises, save lives and secure daily operations
- › **Secapp**








# ARTIFICIAL INTELLIGENCE AND CRIMINALITY

// Ismo Kallioniemi

The rapid development and widespread adoption of AI systems in different industries has brought new opportunities, but at the same time created new challenges for society. One of these challenges is the use of AI for criminal purposes. On the other hand, AI systems can also be used in various criminal investigations and crime prevention.

This article first examines on a general level the potential uses of AI systems for committing crime and crime prevention. After that, the article discusses the crime of forgery in more detail as an example. Finally, the article presents a view of the impact of developments on the prevailing legal situation. 



## USE FOR CRIMINAL PURPOSES

Although AI systems are, in a way, general-purpose technologies, there are some obvious uses for them in the context of crime. These include:

- 1** Phishing scams: AI systems can help create more credible phishing messages by analysing large amounts of personal information and tailoring them to specific targets, making phishing messages more convincing.
- 2** Deepfakes: AI-driven tools can create realistic video and audio products, potentially showing or making individuals appear to say or do things they haven't done. This can be used for extortion, disinformation or identity theft.
- 3** Fraudulent financial transactions: Machine learning can help identify patterns in large amounts of data, which in turn could be used by criminals to find vulnerabilities in digital transfers of funds or optimize the timing of fraudulent transactions and methods to make them harder to detect.
- 4** Harassment and stalking: AI-driven facial recognition tools can be misused to track and monitor individuals without their knowledge or consent, which can be used for stalking or other forms of harassment.
- 5** Identity theft: By analysing large amounts of data, AI can determine the most effective ways to commit identity theft.
- 6** Distribution of drugs and other illegal material: AI can be used to analyse the activities of crime prevention authorities and, for example, to assess which smuggling routes are most difficult to detect.
- 7** Automated hacking: Machine learning algorithms can be used to discover new vulnerabilities or automate attacks, enabling cyberattacks to be carried out more efficiently.
- 8** Cyberbullying and harassment: AI systems can create and send harmful messages or content in large quantities, making cyberbullying campaigns more extensive and harmful.

Of course, AI systems can be used for numerous other criminal purposes, but the above examples illustrate how AI systems can be used for criminal purposes.

## USE OF ARTIFICIAL INTELLIGENCE IN CRIME PREVENTION

Naturally, AI systems can also be used for crime prevention purposes. Such purposes include, but are not limited to:

- 1** Predictive policing: By analysing large amounts of data, AI can help identify potential crime hotspots or times when crimes are likely to occur. This enables a more efficient allocation of police resources.
- 2** Facial recognition systems: When used in public spaces or border control, these systems can identify wanted persons, missing persons or suspects in real time and immediately transmit information to the authorities.
- 3** Shot detection: AI-driven systems such as SoundThinking (formerly ShotSpotter) can detect and locate shootings in real-time, helping police respond faster to firearm-related incidents.
- 4** Fraud detection: Financial institutions use AI systems to detect unusual financial transactions that may indicate fraud, money laundering, or other financial crimes.
- 5** Social Media Surveillance: AI can be used to monitor social media platforms for signs of various extreme behaviours or illegal activities.
- 6** Cybersecurity: AI systems can be used to detect typical patterns of cyberattacks, intrusions, or malware activity and trigger countermeasures when suspicious activity is detected.
- 7** Fight against drug trafficking: AI systems can analyse transport documents and other similar data to predict and identify potential drug trafficking attempts.
- 8** Analysis of videos and other material: When reviewing large amounts of data, such as CCTV videos, AI can quickly detect certain events, objects or persons, drastically reducing the time required for human analysis.



**9** Voice recognition and profiling: In emergency response centres or other telephone lines, AI can analyse sounds or phrases to detect possible abnormalities, such as acting under pressure.

**10** Automated forensics: AI tools can quickly analyse large amounts of electronic evidence to identify facts relevant to the criminal investigation.

As illustrated above, there are obvious applications for AI in crime prevention and forensics. However, despite the promising nature of these applications it is of course necessary to take into account the possible legal limitations associated with their use. However, in an overview article such as this one, the limitations related to the use of AI for crime prevention cannot be examined in full detail.

### FORGERY CRIME AS AN EXAMPLE

In principle, AI systems are capable of detecting regularities in basically any material and once detected, reproducing them in an altered form while maintaining the regularities of the original data. As a result, AI systems can be used to create materials called deepfakes, where, for example, an authentic-looking image of a person created by a computer presents a false verbal message in a video that the perpetrator of the forgery wants it to present. The same applies, of course, to other regularities, such as human handwriting and its characteristics. As is known from forensic handwriting comparisons, human handwriting has numerous regularities, known as shape, movement, direction and use of space, roundness, breaks, gaps, line spacing and the like.

A good example of a forgery created by an AI system is the case discussed in The Wall Street Journal article "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case", in which an AI system falsified the voice of the company's CEO, which was later exploited as a tool for traditional "CEO fraud" by giving the company's finance department a false payment prompt in the CEO's voice. As a result, the company's finance department was misled into making a payment of approximately 200,000 euros to a fictitious subcontractor.

Admittedly, deepfakes such as those illustrated by the CEO fraud example can also be used for non-direct financial purposes. An obvious example would be a harmful deepfake of a politician right before the election date. In this case deepfake might achieve potentially significant societal effects.

### LEGAL IMPLICATIONS

From a legal point of view, crimes committed through AI systems are not, in principle, problematic.

In the case of manslaughter, for example, our legislation does not distinguish between how the perpetrator kills the victim. Legally, it is irrelevant whether the victim is killed with a bladed weapon or by shooting. The same applies to whether the act of deception is committed against a human being or an information system. In this respect, the law is technology neutral.

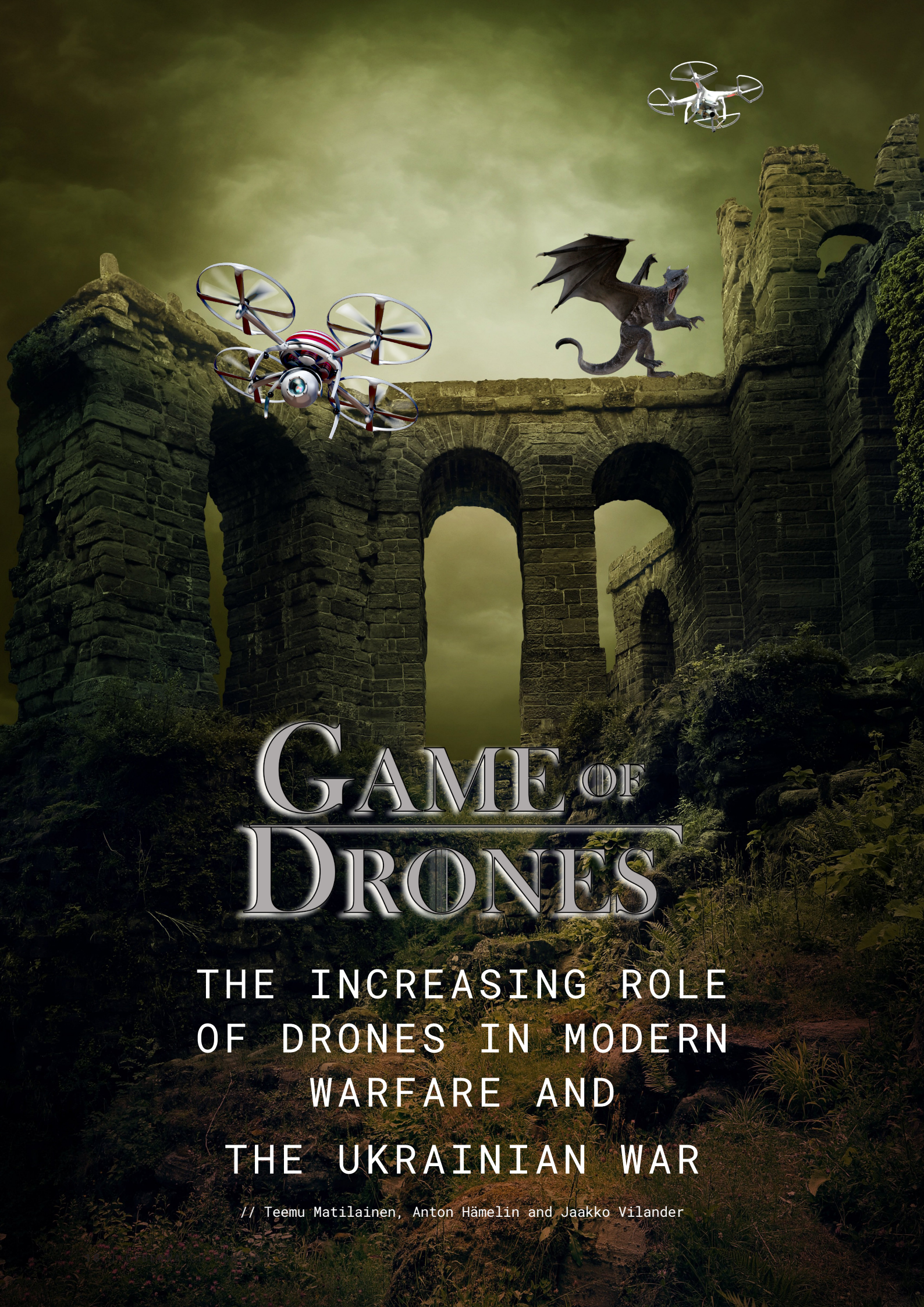
Due to the technological neutrality of our legislation, the examples of criminal uses of AI systems discussed at the beginning of this article are not a legal problem. The impact of AI systems on crime is more of a real problem than a legal problem. AI systems enable many crimes to be carried out in a different way than before, but in essence the crimes remain as they were before. In this respect, the legal framework provided by our existing legislation is also sufficient to regulate crimes committed with AI systems. ■



**ISMO KALLIONIEMI**

- › Attorney Ismo Kallioniemi is specialised in legal issues related to artificial intelligence, demanding trials and related investigations. He is the author of the book "Artificial Intelligence Law - Questions of Property Law and Risk Management" which focuses on legal issues related to artificial intelligence
- › Attorney, partner
- › **Eversheds Attorneys Ltd**





# GAME OF DRONES

THE INCREASING ROLE  
OF DRONES IN MODERN  
WARFARE AND  
THE UKRAINIAN WAR

// Teemu Matilainen, Anton Hämelin and Jaakko Vilander



## ABSTRACT

This article reviews the emerging role of drones and the various forms in which they come to shape war. The examination is conducted against the backdrop of the war in Ukraine, especially after February 24, 2022. As such the conflict in Ukraine represents a notable instance in which Unmanned Aerial Vehicles (UAVs), or hereafter drones, have been strategically employed in warfare, underscoring their integral role in contemporary military operations. While the utilization of drones on the battlefield is multifaceted, their impact extends beyond traditional warfare and frontlines, as demonstrated by attacks on critical infrastructure, such as Ukrainian grain silos and, notably, downtown Moscow.

We contend that the evolution of drone capabilities is intrinsically tied to the advancements in technology, especially artificial intelligence and machine learning, both of which are becoming increasingly pivotal in the development of drone technology. As the capabilities of drones continue to advance and mature, the ongoing development of countermeasures and defensive strategies is also a significant area of technological innovation and research. Simultaneously, Ukraine is serving as a crucible for the future of drone warfare and electronic warfare (EW) capabilities, reflecting their increasingly prominent role in modern warfare. The technological dynamics in Ukraine is likely spark a development that will shape the future of war.

However, technological enthusiasm should not overshadow other aspects of the art of war. Drone warfare comes with critical operational and tactical underpinnings. While drone technology is still in its nascent stages, it has the potential to significantly impact armed conflicts, provided it is integrated effectively with the greater military force. Although glimpses of successful adaptation slowly emerge, this integration remains a formidable challenge

## THE RISE OF THE DRONE

Although the war in Ukraine does not represent the first use of unmanned aerial vehicles in warfare, drones have not played as significant role in the past as they do now. Therefore, the use of drones in Ukraine represents a steep change. Never before have so many drones been used in a military confrontation. For example, the Royal United Services Institute estimates that Ukraine loses about 10,000 drones per month, which itself is indicative of the widespread use of drones. Air defense systems largely neutralize manned aviation, which makes unmanned systems particularly effective (Franke 2023, Hambling 2023).

Not only in the Ukrainian war but for example, the terrorist group ISIS is a good example of the use of

irregular warfare and the effectiveness and efficiency of the brutal tactics used by its followers. In 2014, ISIS took control of Mosul, Iraq's second largest city. In doing so, it made history by becoming the first terrorist organization to use armed drones in combat; drones armed with explosives attacked Iraqis and other coalition forces defending the city. The psychological and physical effects resulted in Iraqi regular army casualties and desertions.

ISIS initially used cheap commercial drones for military purposes for reconnaissance, terrain and surveillance, but later adapted them for offensive operations by attaching improvised explosive devices to them. The use of cheap and commercial drones is understandable because until then only large and well-funded armies could afford armed drones for intelligence, surveillance, target acquisition and reconnaissance (ISTAR) purposes due to the high cost of the technology. However, the use of cheap modified Drones for military purposes by ISIS caused a moment of reckoning, and many militaries and non-military, state and non-state violent actors have begun to consider the possibilities opened up by this industry.

As the world slowly began to look at the defeat of ISIS, eyes turned to the war in Ukraine that broke out in the Donbass. Around the same time in Ukraine, a group of enthusiastic IT professionals voluntarily formed a unit called Aerorozvidka. The group initially started by buying cheap commercial drones and modifying them for military purposes. After two years, in 2016, Aerorozvidka managed to develop its own UAV called R18, and it currently produces several per day and delivers them to various units of the Ukrainian army (Haxhimustafa 2023). Moreover, Ukraine appears to harbor a thriving drone industry as well as a broad range of imports (see table 1). The plains of Ukraine, it seems, seconds as a testbed for drone technology for both defender and aggressor, although Ukraine like had a head start.



References  
on page  
28



**TABLE 1 LIST OF PROBABLE DRONES USED IN UKRAINE (SUPPLEMENTED AND REFINED BASED ON CHAVEZ 2023, P. 8)**

Class	Role	Russia	Ukraine
Military	Combat (UCAV)	Forpost-R Kronstadt Orion "Inokhodets" STC Orlan-10 and -30 Qods Mohajer-6 (IRN) Lastochka-M (lit. Swallow)	A1-CM Furia (lit. Fury) UA Dynamics Punisher Baykar Bayraktar TB2 (TUR)
	Reconnaissance	ZALA 421-series ENICS Eleron-3(SV) Granat-series Izhmash Tachyon Zastava	Ukrspesystems Shark UAV DEVIRO Leleka-100, "Stork" Tupolev 143 (USSR) Skyeton ACS-3 Baykar Bayraktar Mini (TUR) AeroVironment RQ-20 Puma (US) SYPAQ Corvo PPDS (AUS) <sup>1</sup>
	Combat (dropping)		Ukrspesystems PD-1 and -2 Aerorozvidka R18
	Combat (loitering)	ZALA Lancet-3(M) ZALA KUB HESA Shaheed-136 (IRN)	Bober (lit. Beaver) AeroVironment Switchblade 600 (US) AeroVironment Switchblade 300 (US) Aevex Phoenix Ghost (US) RAM II (based on Leleka) WB Electronics Warmate (POL)
Commercial	Various	DJI Mavic (CHN)	DJI Mavic (CHN) DJI Matrice M30T (CHN) Various "dronations"

<sup>1)</sup> The "cardboard drone", which has also been used for combat missions

Known for its agriculture and other heavy industries, Ukraine may not be the most obvious environment for drone innovation. However, the exigencies of the war have turned the country into a sort of cutting-edge invention laboratory, attracting investment from prestigious corporate luminaries. As Deputy Prime Minister of Ukraine Mykhailo Fedorov said in an interview in his office in the capital, Kyiv. "This is a 24/7 technology race. The challenge is that every product in every category has to be changed daily to gain an advantage." More than 200 Ukrainian companies involved in the production of drones are now working hand in hand with frontline military units to adjust and complement drones to improve their ability to kill and spy on the enemy (Hudson & Khudov 2023).

## DRONES AND HOW TO USE THEM

There are multiple uses for drones but use cases can broadly speaking be condensed into three categories: transportation, intelligence, surveillance, and reconnaissance (ISR), and effects. In a military context, transportation drones deliver critical materiel, such as blood transfusion sets, fuel, or batteries, to remote locations with relative ease. As autonomous operation is an exceedingly common feature among even commercial equipment, drones provide a low-risk and low-effort option for surgical logistics. The obvious drawback is, as of now, the usually modest payload capacity, range, and speed. As a means of transportation, drones require the ability to return to base, the optimal solution is a rotary wing model. This offers vertical take-off and landing (VTOL) capability from virtually any surface, but simultaneously places design restrictions that hamper the aforementioned qualities.

Surveillance and intelligence are often the most common uses of drones. All drones carry multi wavelength photo, video, or other data-gathering sensors that allow troops to locate enemy bases, monitor troop movements, and select targets. Drones can also bear sensors for signals intelligence (SIGINT), or more specifically, electronic intelligence (ELINT). Some drones

are known to be equipped with IMEI/IMSI (International Mobile Equipment/Subscriber Identity) catchers, to name an example. Simply put, the height of the sensor equals an expansive radio horizon, which in turn amplifies the utility of drone-borne SIGINT instrumentation. The same principle applies to optical sensors. Thus, drones provide troops with a literal bird's eye view of the battlefield.

The use of ISR drones is especially fruitful in areas such as the plains of Ukraine, where vegetation or geographical obstacles hinder line-of-sight to a comparatively lesser degree. Hence, as Russia's war in Ukraine has demonstrated, drones can be especially valuable, for example, in directing artillery fire or by utilizing the situational picture when attacking in a trench. However, the ISR aspect of drone warfare is not restricted to *in situ* information gathering. Drones may also document attacks, which can provide useful material for various purposes, such as conducting retrospective battle damage assessments or supporting military information operations. In addition, Ukraine has developed its software to enhance geolocation capabilities for artillery, reconnaissance, guidance and command and control purposes. Ukraine's polytechnic program has progressed and improved, but it is still not enough to satisfy its needs (Haxhimustafa 2023).

# FIVE FLAVORS OF COMBAT DRONES

Drones intended for kinetic effects contain two key characteristics: endurance and reuse<sup>2</sup>. Loitering drones, sometimes also loitering munitions, possess enough endurance to hover over the battlefield preying victims, while others support only immediate search-and-destroy type use. Kamikaze drones essentially self-destruct when used, while others use separate ordnance and are recoverable after use. The former are oftentimes military products, while the latter are increasingly commercial – although it is not exclusively so. These two terms are also not mutually exclusive, and although they bear different meanings, they are sometimes used interchangeably. Therefrom rises a third important characteristic, consumer-use, meaning whether the drone is specifically intended for military use or whether it is a commercial, dual-use product.

In this case, we use the reusability, endurance, and consumer-use to delineate kinetic drones into five overarching (yet non-exhaustive and overlapping) categories: Unmanned Combat Aerial Vehicles (UCAV), loitering drones (sometimes also labeled kamikaze drones), military-specific Aerial Explosive Charges (AEC\*), Modified Commercial Drones with an External Ordnance (MCD EO\*), and MCDs with a self-destruct mechanism, i.e., Improvised Explosive Devices (ABIEDs). Broadly speaking, this categorization simultaneously follows a rationale in which the former categories pertain to strategic usage, while the latter variants represent operational and tactical means, as indicated in the table below. Such a categorization may prove useful for military personnel when, i.e., contemplating threat assessments.

<sup>2)</sup> Furthermore, size and operational altitude are other variables provide leeway in drone categorization.

\* These are not previously used designations but useful in dissecting the various variations in kinetic drones.

**TABLE 2 CATEGORIZATION OF DRONES BASED ON REUSABILITY, ENDURANCE AND CONSUMER-USE**

	<b>UCAV</b>	<b>Loitering drone</b>	<b>AEC</b>	<b>MCD-EO</b>	<b>MCD (ABIED)</b>
<b>Reusability</b>	Reusable	Non-reusable	Non-reusable	Reusable	Non-reusable
<b>Endurance</b>	Long to medium	Long to medium	Short	Medium to short	Medium to short
<b>Consumer-use</b>	Non-consumer	Non-consumer	Non-consumer	Consumer	Consumer
	← Strategic				Tactical →

## UNMANNED COMBAT AERIAL VEHICLES

A UCAV, also known as a combat drone, colloquially shortened as drone or battlefield UAV, is an unmanned aerial vehicle (UAV) used for 1) intelligence, surveillance, target acquisition, and reconnaissance but also for 2) combat missions with kinetic effects. A UCAV carries aircraft ordnance such as missiles, e.g., Anti-Tank Guided Missiles (ATGMs), and/or bombs in external hardpoints. These drones are usually under real-time human control, with varying levels of autonomy. Unlike unmanned surveillance and reconnaissance aerial vehicles, UCAVs are used for both drone strikes and battlefield intelligence.

Aircraft of this type have no onboard human pilot. As the operator runs the vehicle from a remote terminal, equipment necessary for a human pilot is not needed, resulting in a lower weight and a smaller size than a manned aircraft. It also relieves the need to consider human constraints related to fatigue, hunger or warmth. Many countries have operational domestic UCAVs, and many more have imported armed drones or are in the process of developing them. Notable producers include the United States, Türkiye, Israel, and China.

Especially Türkiye has become aspired to become a

drone superpower as it challenges China as the world's leading supplier. Sophisticated UAV's such as the Bayraktar TB2 of the MALE (Medium Altitude Long Endurance) classification with its MAM-L ammunition have become nothing short of household names over the course of the war in Ukraine. However, even before, the Bayraktar TB2 has shown its prowess during operations in Syria, where it effectively neutralized Pantsir-S1 and 9K330 Tor air defense systems, and Nagorno-Karabakh, where it decimated tanks, other armored vehicles, and artillery pieces. (Cannon 2022)

However, even the Bayraktar has met its boundaries in Ukraine. While UAVs were responsible for over 70% of Armenian heavy equipment losses in the 2020 Nagorno-Karabakh war, wherein the Strategic Tactical Bayraktar TB2 accounted for up to 63.4 percentage units; in Ukraine, the Bayraktar TB2 has been responsible for less than 1% of Russian heavy equipment losses and has been reduced to an ISR role as the war has progressed due to operational constraints imposed Russian counter capabilities. (Nersisyan & Moore 2023) Moreover, only a small percentage of Bayraktar equipment kills have been main battle tanks (Oryx 2022a).

**References  
on page  
28**





The most notable Russian UCAVs in Ukraine are the Orion and Forpost-R, a licensed copy of the Israeli Aerospace Industries' (IAI) Searcher. In general, Russian UCAV developed has been stagnant, probably due to a preference of attack helicopters. Nevertheless, multiple designs already occupy the conveyor belt. (Oryx 2022c) However, given Russia's recent shortcomings in missile and aircraft development, one should not hold one's breath waiting for Russia to brandish scores of new and operationally feasible UCAVs.

## LOITERING MUNITIONS

A loitering munition (also known as a suicide drone, kamikaze drone, or exploding drone) is a kind of aerial weapon with a built-in munition (warhead), which can loiter (wait passively) around the target area until a target is located; it then attacks the target by crashing into it. Loitering munitions enable faster reaction times against hidden targets that emerge for short periods without placing high-value platforms near the target area and allow more selective targeting as the attack can be changed midflight or aborted altogether.

Loitering munitions fit in the niche between cruise missiles and unmanned combat aerial vehicles (UCAVs or combat drones), sharing characteristics with both. They differ from cruise missiles in that they are designed to loiter for a relatively long time around the target area, and from UCAVs in that a loitering munition is intended to be expended in an attack and has a built-in warhead. As such, they are also non-traditional long-range weapons. In fact, it may well be that Russia's use of long-range loitering drones has exceeded the use of cruise missiles in terms of sheer numbers.

The most popular of these weapons is the Shahed-136, a long-range loitering drone that can fly around like a regular drone and rove within a certain area. These systems are packed with explosives and can be targeted, flown directly at them, and detonated on impact like a missile (Business Insider 2023). However, the real threat arises from its immense range, reportedly exceeding 1 000 km. Since September 2022, Moscow's forces have used them like inexpensive cruise missiles to terrorize cities across Ukraine, often attacking the country's energy grid or civilian infrastructure.

In the medium range, the Russian loitering and self-detonating Lancet-3M has proven highly effective in Ukraine (Nersisyan & Moore 2023). It has been able to damage or destroy various types of highly sophisticated Western equipment far behind the Ukrainian front due to its 40- kilometer range, although it has not been able to

definitively destroy Ukrainian tanks to a significant degree. Documented and confirmed use of the drone by late November 2022 has, according to Oryx (2022b), caused 113 hits and 41 misses, giving it a 73.4% hit rate.

Respectively, Ukraine has had its share of successes with its own arsenal of loitering munitions. The most astounding feat is surely Ukraine's strike using SYPAQ's cardboard drones in a combat role. According to the Kyiv Post, Ukraine struck five fighter aircraft as well as two Pantsir-S1 anti- air missile launchers and the radars of a S-300 air defense systems on Kursk Airfield in August 2023 (Shashkova 2023). Considering that the SYPAQ Corvo costs around 3,500 USD and that fighter jets are valued in the tens of millions, the strike is a manifestation of economy of force. On another quite jolly occasion, a Ukrainian drone nearly struck a Ka-52 attack helicopter mid-flight.

While they are not loitering munitions per se, AECs are worth giving a brief introduction as well. AECs, such as the newly inaugurated Insta Steel Eagle, are a separate category from loitering munitions in that they possess a directional explosive charge, reminiscent of a claymore mine, rather than ramming into the target and detonating upon impact. Conversely, they have a far more modest range, as a VTOL carriage is needed for maneuverability and accuracy. The downsides in range likely render AECs tools best utilized in defensive combat on the platoon or company level and primarily against enemy personnel.

## COMMERCIALY MODIFIED DRONES

For some time, militaries have been using various commercial or consumer quadcopters with varying autonomous capabilities. Minor modifications to their basic systems (i.e., operating systems) allow drones to drop various explosive ordnances. This development has been especially indicative in Ukraine. In fact, quadcopters dropping mortar grenades to have come to represent the most depictive imagery of the war in Ukraine. As technology advances, both sides in Ukraine have begun deploying thousands of racing drones with either external ordnances (MCD-EO) or improvised warheads (ABIED).

MCDs with external ordnances are typically quadcopters as they allow releasing the ordnances in a virtually straight vertical angle, making aiming much easier. However, their low flight altitude and speed make them easy targets for even small arms fire. This is especially the case with heavier payload sizes. At most, projectiles may weigh several kilograms. The same applies to ABIEDs. In some instances, Ukrainians have even attached PM-62 anti-tank mines, typically with a 7.5 kg explosive charge, with grenade fuzing as droppable projectiles.

An ABIED, on the other hand, is fundamentally a commercial version of a kamikaze drone. In other words, the drone itself functions as a warhead that is steered into the target. ABIEDs can therefore benefit from greater speeds and do not necessitate the ability to hover. As a result, ABIEDs are preferably fixed-wing drones. The weapon effect with MCDs usually relies on pressure and fragmentation, but they may also have a directional explosive effect depending on the type of the target. A directional effect reduces payload weight and therefore allows more bang for the buck. In any case, it is important never to approach a downed ABIED. They are highly dangerous until properly handled.

MCDs naturally come with certain drawbacks. First off, due to their weak explosive power and non-existent armor penetration, their principal target is personnel or, with certain caveats, unarmored targets. Additionally, the quality of their sensors may vary. At best, some drones may also be equipped with thermal or night-vision cameras, enabling them to operate in low-light conditions. However, prevailing weather conditions frequently impose limitations on the use of commercial drones. Lastly, insecurity from an ELINT or cyber perspective renders many drones unviable alternatives against a nation-state opponent.

Nevertheless, irregular forces, criminals, and various terrorist organizations frequently utilize commercially modified drones with improvised weapon systems – and with probable success. These perpetrators typically employ them against static targets such as bases, assembly areas, and other installations. However, commercial drones have crept into regular warfare as well. The distinctive feature of the war in Ukraine has specifically been the massive use of fundraised off-the-shelf drones in both combat and recon roles. Moreover, a novel trend in Ukraine has been the introduction of FPV (First Person View) drones, where the live camera feed is relayed directly to specialized goggles worn by the operator. (Nersisyan & Moore 2023)

## SECONDARY EFFECTS OF DRONE USE

However, drone use is not restricted to mere immediate effects. There are implications that drones, combined with swarming tactics, have congested Russian air surveillance capabilities to facilitate the use of secondary munitions, such as long-range missiles or drones. Possible events include the 2022 sinking of the guided missile cruiser Moskva and the 2023 strike on the Russian naval headquarters in Sevastopol. Drones could also be utilized in the same sense as decoys to protect more valuable assets, such as conventional fighter aircraft.

Having the ability to threaten the enemy rear via the air also binds crucial air defense capabilities at a depth relative to the maximum range of the enemy's drone equipment. Moreover, a multitude of drones, with lower altitudes and radar cross-sections, combined with conventional aircraft compels the opposing party to survey a much broader segment of the airspace. Thus, Ukraine's ability to threaten Moscow with drones from the frontline to the Kremlin is a factor that forces Russian military air defense assets to disperse to cover a larger aerial and geographical area. Consecutively, valuable assets such as conventional aircraft need to stage farther from the front to avoid ending up in the crosshairs of Ukraine's drone armada.

The fact that many drones manage to penetrate defensive layers and reach Moscow itself is both a testament of drone efficacy and the shortcomings of Russian air defenses. The brunt of Russia's inland air defenses, largely dependent upon S-400 systems, are designed to counter a nuclear onslaught from beyond the country's borders. As such, Russia's air defense ensemble leaves holes that are penetrable by smaller drones operated from within the country or adjacent to the border. A formidable exhibit of Ukraine's drone capabilities unveiled when it struck multiple targets simultaneously, including Pskov and Moscow; in Pskov, the strike damage at least four Ilyushin-76 transport aircraft (Jeskanen 2023). However, although Ukraine has achieved significant tactical successes, drone strikes alone will almost certainly not be enough to ensure strategic victory.

Even when drones are located, the act of countering them poses another matter. Eliminating rudimentary drones with missile-based systems is hardly cost-effective, as missiles used to eliminate a drone may be significantly more valuable than the drone itself. As a result, utilizing kinetic or fragmenting projectiles is, from an economic perspective, a far more lucrative option. An example of this would be the vehicle-mounted Slinger 160 counter-UAS system delivered to Ukraine. The system's radar can pick up a target of merely 35 cm from distances in excess of 1 km and its 30 mm autocannon ensures fire for effect. (Perttula 2023) SHORAD (Short Range Air Defense) systems introduced after the initial stages of the war in Ukraine have also contributed to eliminating drones (Kallberg 2022).





Ukraine has also procured six anti-drone defense systems known as the "Shahed Hunter", a name that refers to the types of Iranian-made drones used by Russian forces. Shahed Hunter is a combination of radar and signal jamming that can detect an enemy drone up to 40 kilometers away from the target. It detects and intercepts enemy drones, unleashing Interceptor drones that use heavy netting to intercept enemy UAVs in the air. The net captures the drone and releases a parachute that slows it down and allows for a soft landing in the safest way without explosions or casualties. Shahed Hunters are already for example protecting critical energy plants in Ukraine (United24 2023; Business Insider 2023).

However, the most feasible counter-weapons against drones are non-kinetic. One plausible vein in this regard concerns Directed-Energy Weapons (DEW). The idea with DEWs is to target a designated object with sufficient energy, such as a laser, microwave radiation or a particle beam, to cause damage. DEW effects can thus be affordable and instantaneous, which makes target acquisition and effects much more straightforward. An application of this kind is the Raytheon 50- kw High Energy Laser (HEL), which reportedly possesses the capability to knock out, amongst other airborne objects, drones (Osborn, 2023). However, DEW technology is still in its developmental stage. On the contrary, EW capabilities, which are relatively plenty in the Russian Armed Forces, have shown their prowess in countering the growing aerial threat.

## ELECTRONIC WARFARE AGAINST DRONES

Electronic Warfare (EW) refers to reconnaissance and jamming of systems using electromagnetic radiation and their countermeasures. Today, regardless of the level of equipment or tactics of a military force, everyone uses radios, command systems and weapon systems that emit electromagnetic radiation. Electronic warfare forces are an integral part of modern warfare. Electronic intelligence and surveillance reveal the activities of enemy forces and weapon systems on land, sea and air (The Finnish Defence Forces 2022).

While most sensors are passive, drones themselves require a downlink if operated in real-time. This makes both drones and ground stations themselves susceptible to targeting via ELINT. In such a scenario, threat to personnel can be countered by separating the user interface, i.e., the operator, and the antenna. EW can also be used to

disrupt or neutralize drones' communication, navigation and control systems. Drones operate efficiently on a variety of signals, including radio frequency (RF) transmissions, GPS, and other wireless technologies. Various electronic warfare techniques work to jam these signals, making it difficult or impossible for the drone to receive commands, maintain control, or navigate precisely. (Noreika 2023; Kallberg 2022)

Jamming has always been a problem especially when using quadcopters because consumer drone controllers operate on known, legally controlled frequency bands. In this case, the jammer only needs to transmit strong enough noise at the same frequency as the drone controller operates, in which case the drone's control signal is lost due to a static snowstorm and stops responding. As the war has progressed, Russia, for example, has introduced increasingly powerful and sophisticated jamming devices to target drones that directed artillery fire at their positions and dropped grenades into their trenches (Hambling 2023). The traditional recipe for jamming in radio communications has been frequency hopping, which broadens the frequency that must be affected to overpower the signal. However, there are other options too.

During the war, the parties have also started to utilize solutions based on artificial intelligence (AI) technology. AI-based software may, for instance, stabilize the drone despite electronic interference and keep it locked to a predefined target, even if the target is moving. This can be considered a significant improvement compared to existing drones that track specific coordinates. The AI-based software offers an upgrade especially to Ukraine's arsenal of affordable yet jam susceptible FPV drones. If the drone loses contact with its pilot and the target is locked, the AI system takes control. The sensors on the drone recognize the object's physical characteristics and adjust the aircraft's flight path accordingly, reaching the acquired target. However, it still requires a human operator to select the target on which the drone strike is to be carried out (Hudson & Khudov 2023).



Artificial intelligence already plays a key role in increasing the autonomy of unmanned systems with the help of machine learning and big data. Autonomy improves the functionality of drones, which enables more accurate observation and airstrikes. However, AI-controlled drones are only as good as the algorithms they work with and the data from which they are fed, so it remains to be seen whether their added value in the short term will remain only at the tactical level (Rogers & Kunertova 2022, p. 8). Affordable drones also enable swarming tactics, if even rudimentarily. This means that jammers would also potentially have to be spread over a substantial area to mount an effective drone defense. Thus, jamming devices alone cannot reliably combat the threat of affordable, potentially autonomous wandering missiles and small drones (Kunertova 2022, p. 4).

### THE DRONE WARS

Innovations in the use of drones during the war in Ukraine imply further ramifications for the public image of armed drones and increased proliferation control. The mainly commercial origin of the dual-use components of drone systems and the participation of the private sector are two very significant factors. Voluntary actors and various crowdfunding campaigns have also strengthened the participation of civilians in military operations. Both Russian and Ukrainian forces have acquired some of their drone capability by "droning" small hobbyist drones from the local population. Charities that raise money to buy fighter jets, such as Ukraine's Prytula Foundation and Come Back Alive, may be directly involved with the arms industry. This support from the private sector in part normalizes the use of drones carrying explosives (Kunertova 2022 p. 3).

All this underscores the ongoing transition where it is now the population who supplements the military with cutting-edge technology instead of the other way around. A drone is now one of many gadgets (think smartphones, vehicles, computers etc.) a citizen can provide for the warring nation. One can imagine what possibilities this setup may entail for a country with a vast reservist force, such as Finland or Israel.

To a similar end, Ukraine implements the "Army of Drones" program, which aims to maximize the use of reconnaissance and attack drones by Kiev to compensate for Russia's great advantage in air and artillery power. The program has helped private companies train more than 10,000 drone operators in the past year, with the goal of training 10,000 more in the next six months. In July 2022, the Ukrainian World Congress (UWC) and the Ministry of Digital Transformation of Ukraine signed a Memorandum of Cooperation to support the UNITED24 fundraising platform for the "Army of Drones" project. This program involves drone procurement, delivery, maintenance and replacement, as well as pilot training (Ukrainian World Congress 2022). Ukrainian President Zelenskyy said in his May 5 speech to mark the first anniversary of the UNITED24 platform that the platform has already raised more than 330 million USD from people in more than 100 countries (United24 2023; Business Insider 2023).

As if to highlight the current paradigm shift, in the sky of Ukraine, a new era is emerging in aerial warfare: a drone-on-drone battle, where different drones are already at war against each other. No bullets, missiles or bombs are used in these dogfights. Some hobbyist camera quadcopters, used to spy on enemy positions, simply ram each other in a brutal aerial demolition derby. In other encounters, highly sophisticated ships use advanced radar – backed by artificial intelligence and the latest avionics – to launch precise fire nets that intercept other drones. (Sherman 2023).



References  
on page  
28







## CONCLUSION

In recent years, Ukraine has become an important place in drone development and manufacturing. Joint partnerships and effective cooperation between the private and public sectors have led to the development or reuse of Drones for military use. The innovation pressure caused by the war, the ingenuity of the Ukrainian people and the opportunity to cooperate closely with many experts from Western countries have helped to create a solid foundation for the domestic defense industry. In the future, the Ukrainian drone industry will most likely be a serious international player capable of exporting combat-proven systems (Franke 2023).

The crucial question pestering military planners and analysts, however, concerns the actual effectiveness of drone warfare. At the time, this is likely to remain an unsolved mystery. While there is data, even open-source

data, on successful drone strikes, no credible data of the ratio of successful drone strikes to the total amount of attempted drone strikes currently exists. Therefore, the effectiveness of drones is a highly circumstantial matter and affected by a multitude of intermediary factors, e.g., overall troop composition and force structure, the character of the conflict, terrain, and available resources for each party involved. The hi-tech extravaganza of the war in Ukraine vis-à-vis Nagorno-Karabakh may provide some explanatory power to the discrepancies between the two wars, although Armenian air defenses were hardly a strainer either (Cannon 2023).

The war in Ukraine nonetheless confirms that drones are becoming stealthier, speedier, smaller, more lethal, more easily operable, and arrive in the hands of more actors. They are also utilized in exceedingly ingenious

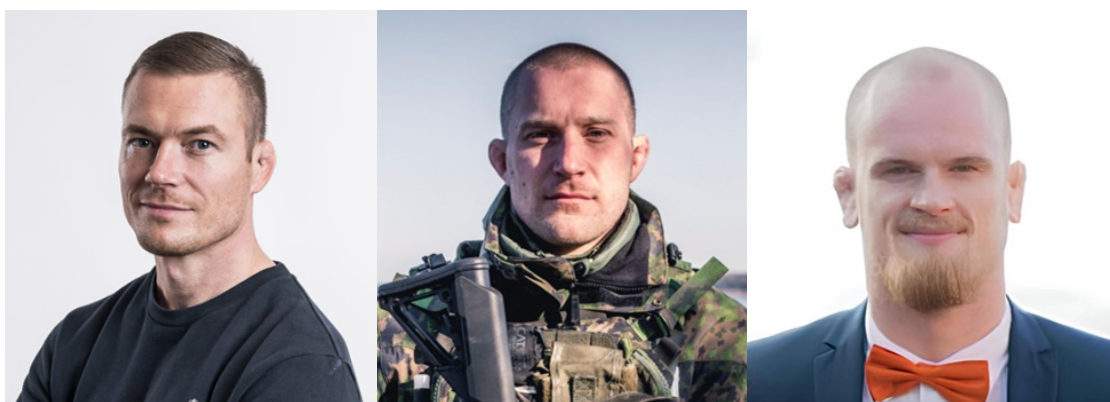
ways. The war shows that drones can achieve different effects depending on the type of platform and its payload. While large missile-carrying drones can be devastating, especially in air superiority situations, smaller drones have proven critical for situational awareness of infantry, control units, and artillery targeting. Moreover, the deployment of dropped projectiles presents a challenging and less easily defensible method for delivering explosive payloads (Kunertova 2022, p. 2).

The innovation pressure caused by the war will also show what the development of technology can achieve in drone operation in the years to come. In any case, it is certain that electronic warfare and drone operations is playing and will play an increasingly large part in modern warfare – as Ukraine has witnessed. It is entirely possible that drones and EW capabilities will usher another cat-and-mouse game reminiscent of the classic competition of armor and anti-tank weapons. The ongoing war in Ukraine has and will surely still greatly accelerate the development of both these facets and shape the wars to come. Different categories of drones will emerge and, as a result, future wars will likely witness systems ranging for miniature commercial equipment to full-fledged autonomous fighter jets.

However, drone warfare is still very much in its infancy. While drones provide advantages in various contemporary armed conflicts, translating technological or even tactical ingenuity into operational success is an

entirely different conundrum. As Kallberg (2022) frankly states, tanks, not drones, will liberate Ukraine. Although we have hints of successful combined use of drone and land power in Nagorno-Karabakh for instance, how to incorporate drones into maneuverist, combined arms warfare unearths a largely unresolved problem set – especially if air superiority is not guaranteed. Therefore, drones is an evolution, not a revolution, in warfare. However, drones can provide crucial support if properly deployed in lieu of troops with operational maneuverability and armor. In this formula, drones may provide Close Air Support (CAS), overwatch, or intelligence in various forms. In a sense, drones may herald the second coming of Army aviation.

However, that is not the sole observation that offers some perspective as to the developmental stage of drone warfare. As a matter of fact, the use of drones in Ukraine shares, in many ways, semblance with the introduction aircraft in the Great War. Their primary use revolves around their ISR function, just as the biplane in the early 20th century. Their use in the effects function is primarily restricted to rudimentary approaches, such as dropping grenades with contact fuzing. Albeit introduced at a later stage, the original kamikaze planes were the offspring of the same era, namely World War II. One can even observe similarities in the psychological realm. Now, the dreaded shriek of dive bombers has been replaced by the ominously foreboding hum of the commercial quadcopter, the harbinger of destruction. ■



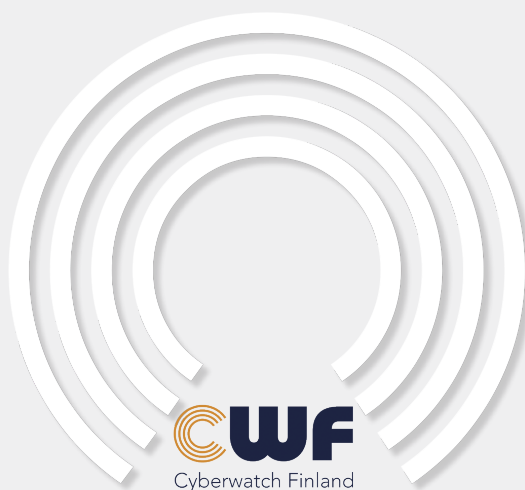
TEEMU MATILAINEN, ANTON HÄMELIN, JAAKKO VILANDER

Authors have years of experience from various assignments and roles on the field of security. In addition to operating in Finland, the authors have served in variety of international roles.



## REFERENCES

- Ali Haxhimustafa 2023. From ISIS to Ukraine: The Evolution of Drones' Use On The Battlefield. Published 31.7.2023. <https://www.thedefencehorizon.org/amp/evolution-drones-ukraine-isis>.
- Alius Noreika 2023, Ukraine is Seeking Electronic Warfare Equipment to Counter Lancet Drones. Technology org. Published 3.7.2023. <https://www.technology.org/2023/07/03/ukraine-electronic-warfare-to-counter-lancet-drones/>.
- Business Insider 2023. A Ukrainian donation drive built an 'Army of Drones' and picked up an unusual system called a 'Shahed Hunter' for Kyiv's forces. Published 11.5.2023. <https://www.businessinsider.com/ukraine-army-of-drones-shahed-hunters-donation-push-2023-5?r=US&IR=T>.
- Brendon J. Cannon 2022. Turkey's rise as a drone power: trial by fire. Defense and Security Analysis, pp. 1–20. DOI: 10.1080/14751798.2022.2068562
- David Hambling 2023, New Report: Ukraine Drone Losses Are '10,000 Per Month'. Forbes. Published 22.5.2023. <https://www.forbes.com/sites/davidhambling/2023/05/22/ukraine-drones-losses-are-10000-per-month/>.
- Dominika Kunertova 2022. The Ukraine Drone Effect on European Militaries. Center for Security Studies (CSS). Published 2022. [https://css.ethz.ch/content/dam/ethz/special/interest/gess/cis/center-for-securities-studies/pdfs/PP10-15\\_2022-EN.pdf](https://css.ethz.ch/content/dam/ethz/special/interest/gess/cis/center-for-securities-studies/pdfs/PP10-15_2022-EN.pdf).
- Jan Kallberg. Drones Will not Liberate Ukraine – but Tanks Will. Center for European Policy Analysis (CEPA). <https://cepa.org/drones-will-not-liberate-ukraine-but-tanks-will/>.
- James Rogers & Dominika Kunertova 2022. The Vulnerabilities of the Drone Age Established Threats and Emerging Issues out to 2035. Center for war studies. Published 2022. [https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/NATO\\_VDA\\_Policy\\_Report.pdf](https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/NATO_VDA_Policy_Report.pdf).
- Jason Sherman 2023. Drone-on-Drone Combat in Ukraine Marks a New Era of Aerial Warfare. Scientific American. Published 3.4.2023. <https://www.scientificamerican.com/article/drone-on-drone-combat-in-ukraine-marks-a-new-era-of-aerial-warfare/>.
- Jenni Jeskanen 1.9.2023. Venäjän ilma-torjunta "ei pysty selviämään tehtävistään edes hyvällä tasolla", sanoo sotilas-asiantuntija. Ulkomaat, Helsingin Sanomat. <https://www.hs.fi/ulkomaat/art-200009820525.html>.
- John Hudson and Kostiantyn Khudov 2023. The war in Ukraine is spurring a revolution in drone warfare using AI. The Washington post. Published 26.6.2023. <https://www.washingtonpost.com/world/2023/07/26/drones-ai-ukraine-war-innovation/>.
- Kerry Chávez 2023. Learning on the Fly: Drones in the Russian-Ukrainian War. Arms Control Today, January-February. <https://www.armscontrol.org/act/2023-01/features/learning-fly-drones-russian-ukrainian-war>.
- Kris Osborne 28.8.2023. Laser-Armed, Drone Killing Strykers Bring Army New Attack Tactics. Warrior Maven, Center for Military Modernization. <https://warriormaven.com/land/laser-armed-drone-killing-strykers-bring-army-new-attack-tactics>.
- Leonid Nersisyan & Cerwyn Moore 2023. Comparing Russo-Ukrainian war and Second Karabakh war: performance and failures. In Pentti Forsström (ed.). Russia's war on Ukraine – Strategic and operational designs and implementation, p. 78-86. Department of Warfare, National Defence University. Tampere: Punamusta. (Unpublished)
- Maryna Shashkova 27.8.2023. Kyiv Claims 5 Russian Fighter Jets Hit in Drone Attack on Kursk Airfield. Kyiv Post. <https://www.kyivpost.com/post/20973>.
- Oryx 25.3.2022a. Defending Ukraine - Listing Russian Military Equipment Destroyed By Bayraktar TB2s. Oryx Spioenkop. <https://www.oryxspioenkop.com/2022/02/defending-ukraine-listing-russian-army.html>.
- Oryx 25.11.2022b. Hit or Miss: The Russian Loitering Munition Kill List. Oryx Spioenkop. <https://www.oryxspioenkop.com/2022/11/hit-or-miss-russian-loitering-munition.html>.
- Oryx 7.4.2022c. Nascent Capabilities: Russian Armed Drones Over Ukraine. Oryx Spioenkop. <https://www.oryxspioenkop.com/2022/04/nascent-capabilities-russian-armed.html>.
- The Finnish Defence forces 2022. Elektroninen sodankäynti suojaa, paljastaa ja hyökkää keihään kärjessä. Published 5.5.2022. <https://maavoimat.fi/-/elektroninen-sodankaynti-suojaa-paljastaa-ja-hyokkaa-keihaan-karjessa->.
- Ukrainian World Congress 2022. UWC IS PARTNERING WITH THE UKRAINIAN MINISTRY OF DIGITAL TRANSFORMATION TO BUILD AN ARMY OF DRONES FOR UKRAINE. Published 2022. <https://www.ukrainianworldcongress.org/united24/>.
- Ulrike Franke 2023. Drones in Ukraine and beyond: Everything you need to know. The European Council on Foreign Relations (ECFR). Published 11.8.2023. <https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know/>.
- United24 2023. 'SHAHED HUNTER': FIRST ANTI-DRONE SYSTEMS NOW INSTALLED AT CRITICAL INFRASTRUCTURE FACILITIES. Published 27.01.2023. [https://u24.gov.ua/news/shahed\\_hunters\\_defenders](https://u24.gov.ua/news/shahed_hunters_defenders).
- Pentti Perttula 8.9.2023. Tämä ilmatorjuntatykki osuu drooniin yhdellä laukauksella. Verkkouutiset. [https://www.verkkouutiset.fi/a/tama-ilmatorjuntatykki-osuu-drooniin-yhdella-laukauksella/?ref=rns\\_tw#1e9](https://www.verkkouutiset.fi/a/tama-ilmatorjuntatykki-osuu-drooniin-yhdella-laukauksella/?ref=rns_tw#1e9).





# THE CYBER COMPETENCE OF THE COMPANY'S PERSONNEL DEVELOPS THROUGH CYBER MASTER COURSES

// Pertti Kuokkanen

Over the past two years, more than 120 cyber experts have been trained in cooperation with MIF for companies and public administration organisations. Training has come in handy and has been found to meet the challenge required by the current continuous change in the operating environment. The form of education has been specialist vocational qualifications lasting more than one year.



## THE ACCELERATING CHANGE IN THE CYBER ENVIRONMENT POSES CHALLENGES TO COMPETENCE

The change in the operating environment challenges companies and public administration organisations both functionally and formally to develop the competence of their personnel. Responding to various cybersecurity threats, managing business continuity, and regulating society create new needs and requirements for the safe implementation of core activities and thus also for the training of personnel.

As networked digitalisation expands, buyers of services and goods will increasingly express concern about whether cooperation with a company or service organisation increases their cyber risk. In addition to this, the financial concern is related to the potential major damage that could be caused by cyber failures. Criminals are increasingly targeting large companies through smaller partners. Supply chain analysis is emerging as a significant component of risk management.

Under the guidance of society, the EU's CER and NIS2 directives, for example, impose new obligations on the operations of companies and organisations. The CER Directive sets out harmonised minimum requirements to safeguard the provision of essential services in the EU internal market and increase the resilience of critical entities. It emphasises a risk-based approach to ensure operational security against a wide range of threats: natural hazards, terrorist attacks, insider threats or sabotage, all of which may have cybersecurity or other related factors. The aim of the NIS2 Directive is to improve the basic level of cybersecurity in the EU and ensure the continuity of critical entities. It includes requirements for operating principles, case handling processes, supply chain security, basic cyber hygiene practices and cybersecurity training, among other things.

From a competence perspective, companies and organisations must define the competence requirements for their personnel's cyber competence, ensure their accessibility based on appropriate education, training, or experience, acquire the required qualifications, and evaluate the effectiveness of the measures taken. Appropriate documented information shall be kept on all this as evidence of competence. Practical ways of obtaining qualifications may include, for example, training, mentoring, or transferring existing employees, or hiring or renting qualified persons.

## COMPANY TRAINING PROGRAMS TO MEET REQUIREMENTS

An up-to-date training programme ensures regular maintenance of knowledge and skills and considers the requirements of the changing operating environment. The level of training should be assessed by regular exercises or tests.

The state of a company's cyber competence can be tentatively outlined by answering simple questions such as:

- Will the company's new employees receive sufficient orientation training in the company's digitalisation and its security?
- Does the company have a regular training and exercise programme used to update their skills and knowledge regarding the latest threats and trends (development of situational awareness)?
- Does the personnel's competence meet the requirements of the NIS2 directive?

Building competence and its up-to-date implementation are based on the operational goals of the company or organisation. When arranging training, it is a good idea to carefully go through the following list of things to ensure, for example:

- The skills needed to reach the company's goals and manage the risks have been specified.
- The capabilities and skill levels required by the work tasks have been defined as a basis for planning the training.
- Employees must be provided resilience-related skills in accordance with their duties.
- A training programme ensures regular maintenance of the skills and knowledge, taking account of the requirements set by the changing operating environment.
- The training programme includes the company's operating models for continuity as well as operating models for exceptional circumstances and the use of technologies.
- The level of training is assessed in regular exercises.
- The company's management understands competence development as part of cyber responsibility.



**The whole domain is really interesting, and I will continue to improve and develop my own knowledge. Network vulnerabilities and data leaks are always topical in working life, and these should be reviewed annually."**

Students' personal feedback from courses that ended in spring 2023.

## CYBER MASTER TRAINING DEVELOPS CYBER SKILLS

The aim of the Cyber Master -degree programme is to broaden the understanding of the multidimensional threats and means of cybersecurity in order to secure the operations of the organisation and manage possible disruptions. Training is divided into two different levels as follows:

1. The Specialist Qualification in Product Development / Cyber Master is intended for people who have the opportunity to develop the cybersecurity of an organisation and take ideas forward to be applied on a practical level. The training is primarily intended for designers and service designers.
2. The Specialist Qualification in Management and Business Management / Cyber Master is intended for individuals who have the opportunity to decide and/or develop the cybersecurity of an organisation and take ideas forward for application. The training is primarily intended for persons working in the organisation's management team.

Cybersecurity is built on the ability to understand, identify, and increase the cybersecurity and personnel competence of a company or organisation. During the program, the company's ability, and sustainability to face the growing challenges of cybersecurity are developed and built through measures for analysing the operating environment, risk management and continuity planning.

Cybersecurity is much more than security and protection; It means observation, anticipation, the ability to react and timely communication to prevent cyber operations. The development of cybersecurity increases the proactive ability of the entire company to withstand exceptional and disruptive factors and to manage crisis situations. With the help of the training programme, the lessons learned in the training are put directly into practice. Implementing the result of the training at the latest at the end of the course and also after it is very important from the perspective of building a company's cyber culture. In this context, the role of the student's mentor is significantly emphasised. The development contribution of the course is directly targeted at the operations of a company or organisation. During the training, the student completes a specialist vocational qualification.



## TEACHING MODULES

The content of the course is structured according to the principle of four workshops as follows:

**Workshop 1:** Teaches the necessary concepts and provides the basis for the measures by which the participant is able to determine the current state, operational readiness and continuous improvement of the student's own organisation and create a basis for development work. The result is an analysis of the operating environment.

**Workshop 2:** The aim is to develop own information security skills and determine your organisation's ability to detect, prevent, mitigate and respond to changing cyber threats, as well as to conduct a cyber risk analysis of your organisation/area of responsibility.

**Workshop 3:** Structure and draft of the organisation's cybersecurity strategy/operating model - vision and development activities. Follow-up actions required for cybersecurity and development based on the organisation's objectives and vision. Interfaces with the organisation's business strategy and contingency plan.

**Workshop 4:** Operational level plan for the most urgent measures to improve cybersecurity. These measures create the conditions for the implementation of the strategy and are part of continuity management measures. Also includes communication, cyber hygiene and continuous improvement.

Each workshop consists of 2-3 teaching periods, which provide the basics of the chosen topics, self-study material and assignments. The tasks are carried out in the company's or organisation's own operating environment. These works aim to maximize the benefits for both the student and the company. Some of the periods will be implemented as classroom teaching and some as distance learning.

This training program can also be customised into shorter company- or organisation-specific programs. The modular structure and content of the program can be modified to meet the customer's needs and scope.



**In general, there is a need for product development in information security and general use. Be able to productise needs well for the management team in order to open the purse strings to important matters!**

Students' personal feedback from courses that ended in spring 2023.





## COMPETENCE AIMS FOR A FLEXIBLE AND DEVELOPING CYBER CULTURE

It is in the company's interest that the company has and develops a good cyber culture, consisting of practices related to digitalisation, work ethic, common rules and conditions, and ways of interaction between employees. Only through competence development and implementation can this goal be achieved.

Dear Reader, when you've come this far, ask yourself:

- Has it been ensured that the employees feel that they can influence the company's digitalisation and cybersecurity and that they have the opportunity to bring up shortcomings related to them?
- Are the members of the board of directors and the management team committed to decisions on digital and cybersecurity, do they personally comply with them, and do they bring up inefficient practices in cooperation with the employees?
- Has it been ensured that the organisation talks openly and positively to the personnel on why digital and cybersecurity is important?

If you are still unsure after this, make sure of the following:

- A good safety culture in the company consists of the operating methods related to digitalisation, work morale, joint rules and conditions and the ways employees interact with each other.
- The changes brought by digitalisation and cybersecurity have been processed amicably, covering the joint goals, work tasks and areas of responsibility as well as the rules and operating methods.

”

Perhaps one of the essential insights gained through the training is how the management sees things and how views can be influenced, and on the development stories day, the matter was also discussed well and more insight.

Students' personal feedback from courses that ended in spring 2023.

- The personnel of the company
  - know-how and to whom to report problems or incidents. They also feel that they are encouraged to report.
  - are not afraid of negative consequences when reporting problems or incidents.
  - feel that they can question operating models constructively; the skills, abilities and creativity of the personnel are utilised.
  - feel that the insights are genuinely utilised in the planning and transformation of digital and cybersecurity practices.
  - understand the importance of digital and cybersecurity and their importance to the organisation. A learning and developing work community is taken into account; smooth cooperation and being active are encouraged.
- Instead of failures, the reporting and internal communications focus on successes (for instance, the number of people who reported phishing messages is stated instead of the number of those who fell for them).
- Time for social interaction is provided.

If functional deviations arose because of reviewing tasks, develop your company's or organisation's cyber competence at all levels and in all task roles. If necessary, please contact us, we will arrange training and support you. ■

Ask for more information:  
myynti@cyberwatchfinland.fi  
Phone:  
Ake +358 45 343 6500



**PERTTI KUOKKANEN**

- ' Senior Adviser, Head Instructor
- ' Colonel (ret.), Ph.D.
- ' Cyberwatch Finland



# THE WAR IN UKRAINE IS ALSO A QUESTION OF INFORMATION- AND CYBER DOMINANCE

// Josef Schroefl and Soenke Marahrens





## BACKGROUND INFORMATION

On the morning of February 24, 2022<sup>1</sup>, Russia's attack on Ukraine suddenly catapulted the West into a reality it hadn't realised until then. Since then, especially the larger Western states have been forced to leave a state of self-deception that they have cultivated. In the meantime, other perspectives have become familiar to them. The Russian president has always denied the murders, the poison attacks, and the many attacks on our western value system, for which he has used his "truth" as a perfidious disruptive strategy. That "truth" was coherently messaged in and of itself: Russia is always innocent of everything the West attributes to that country. Putin's mission is to save Russia and the Russian people from destruction because the West wants to destroy Russia.

The invasion of Ukraine cannot be understood without Putin's view of history. In his view, Russia had to assert itself against enemies from the West for 1000 years and thereby gained its strength - most recently in Second World War. Putin accuses the West of denying Russia's world power status since 1990<sup>2</sup>.

To pursue his goals, Putin has merely reactivated the old methods from the KGB junk room. The "old" Soviet instruments included:

- Dis- and misinformation: Fake news must be spread on all possible channels. In recent years, the Kremlin has also built up its own media industry with RT and Sputnik to influence opinion abroad. A specialty of the Soviet as well as current Russian disinformation is the reinterpretation of real or historical events.
- Sabotage: The goal is to confuse the enemy and destabilise the enemy's population trust in the government's ability to guarantee the basic needs of life. State actors work closely with organised crime, which is a general feature of Russian warfare<sup>3</sup>.

In contrast to the Soviet era, however, new, and additional "digital fire accelerators" are available to him in the form of the Internet and social networks. In our times that means, the Russians are conducting an ever more intense cyber and information war, including the electromagnetic spectrum: The systematic distribution of psychologically and ideologically grounded material with provocative character and a mixture of partly truthful and false information accompanied by attacks on the critical infrastructure can create mass psychosis, to despair and a mood of doom and undermine confidence (of those attacked) in their government and armed forces.

## THE INTERDEPENDENCE OF CYBER- AND INFORMATION WAR

Cyber war is on the one hand the military conflict in and around virtual space, cyberspace, and includes all measures of information and communication technology security as well as all measures to ward off sovereignty-endangering cyberattacks. Endangering sovereignty may be cyberattacks on military ICT systems as well as on critical infrastructures and / or constitutional institutions.

On the other hand, cyber war refers to the high-tech forms of war in the information age, which are based on extensive computerisation, electronisation and networking of almost all civil and military areas and concerns. That means, that the battle for (the right) information - including information warfare - takes mainly place in cyberspace. The manifestations of information war are known as deepfakes, dis- and misinformation campaigns and -operations as well as psychological operations (PsyOps). And all of that can be interrupted or disturbed via the electromagnetic spectrum, fe. by attacking satellite communications.

But cyberspace offers also defensive options: false and/or dis- and misinformation can also be countered by means of the Internet. As excellently demonstrated by Gen Nakasone's US CyberCommand during the US elections last year, when dozens of social media accounts on Twitter, Instagram, etc. were simply shut down using military Computer Network Attacks<sup>4</sup>.

The same can also be seen in the current war in Ukraine: common cyberattacks such as ransomware, DDoS attacks, use of crypto apps, malware, compromise of information systems, 0-day cross-platform worms, SCADA attacks, etc. were used by both sides, to influence the enemy, cause damage or repel.

If you want to understand how Russian citizens see the world, you must speak Russian and watch Russian TV. Kremlin control permeates every part of Russian TV. During the day there are no more soaps or series, just hard-hitting propaganda about Russia's place in the world, the threat posed by the liberal but weak West and the "liberation" of the Ukraine from Nazi s. "The Bandera elites must be liquidated; they cannot be re-educated. The societal swamp that supported them must experience the terror of war, learn the lesson, and pay for its guilt."<sup>5</sup> was and is still one of the main messages from Russia and serves the narrative "Threatened Values".

That narrative is also used to criticise progressive Western values such as the rights of women, ethnic and religious minorities, or the LGBTQ community. According to pro-Kremlin disinformation outlets, the western world is destroying fundamental values through decadence, feminism, and political over-correctness. Russia, on the other hand, is the guardian of decency and morals<sup>6</sup>.

The electromagnetic spectrum has been used for interfering and/or disrupting the adversaries' flow of information. Russia tried to cut the cyber space within the Ukraine by shooting down their server and mobile connections like 3G/4G-band, to disturb their national command- and control systems and that the Ukraine cannot reply on Russian dis- and misinformation.

One of the main intents of Russian propaganda activities is to “dehumanize” the other side. Targeted means of influencing serve as part of psychological warfare, a common method in times of war. These narratives<sup>7</sup> determine how and what the West should think about a crisis/war and what judgment must be made. Many agree that Ukraine's conflict with Russia — an established cyber superpower that isn't hesitant about flexing its muscle aggressively — could test the rules of war in new and unexpected ways. Some say it already has<sup>8</sup>.

Cyber is the new battlefield and its means like information-operations could be as hard powers as military means, although NATO and EU and their member states are still not clear on this either. Is it one new comprehensive domain or maybe is it better to regard them separately<sup>9</sup>.

The electromagnetic spectrum, information-, and cyberspace reside within the physical dimensions of the information environment and can be used as sites of warfare, equivalent and akin to the domains of land, air, sea, and space.

These domains are of equal value, whereby it must always be considered that one can influence the other and that information- or electromagnetic attacks cannot be that successful without using cyberspace<sup>10</sup>. The connection between can also be summarized with a comparison: It's a threaded pipe in which water flows. The thread is the electromagnetic spectrum, the pipe is the cyberspace, and the water represents the information flowing in it<sup>11</sup>. The electromagnetic spectrum cannot therefore fully be separated from the cyber- and information space.

## THE ELECTROMAGNETIC WARFARE

There is also an invisible battle for radio dominance ongoing. Both sides are trying to block the opponent's radio and radar systems. Still, with advantages for the Ukrainian side, since they, among other things, have used cyberattacks to disable Russian drones, which pose as Russian fighter jets by using false identifiers, and in some cases, they have even been able to take control over drones<sup>12</sup>.

But why and how is the electromagnetic spectrum and the Internet in the Ukraine still existing, - why hasn't it been destroyed by Russia?

First, - Starlink, a company of the US-American business magnate Elon Musk, which offers Internet access

via its satellite network, comes into place. Several thousand Starlink terminals are currently in use within the Ukraine to support and maintain the local mobile network. Even Elon Musk recently publicly rolled out the idea of turning off the system again because it would cost him, the richest man in the world, an enormous amount. He also posted a peace plan for Ukraine on Twitter, which must have caused extremely satisfied faces in Moscow. In it he suggested that Crimea should remain with Russia (“that was Khrushchev's fault,” he argued) and that the people of Donbass should vote whether they would rather belong to Russia or Ukraine. Some days later he denied. His satellite network is still working and paid by him<sup>13</sup>.

Second, - because on the day of the invasion (24th of February) – three long planned key decisions took place:

1. The Ukrainian Telecom regulator (NKRZI) had allocated the Ukrainian operators additional 3G and 4G frequency bands. That increase of frequencies meant that the whole country benefited from that extra capacity, especially during the first wave of refugees.
2. The Ukrainian mobile operators and the Telecom companies decided not to suspend any account if it would run out of credit. That meant, that all soldiers (but also refugees and the population at all) has always been able to communicate, - fe. with their families.
3. All Ukrainian mobile operators and the NKRZI, suspended all inbound roamers from Russia and Belarus. That meant, that Russian and Belarussian mobile networks could not be used for roaming anymore.

All these are key reasons, why Russia hasn't yet disrupted Ukraine's cellphone network and internet, neither with hacking nor bombing. Russian soldiers need it for their communication as well! Smartphones can be found with all soldiers involved in the war. But cellphones are pinging signals to the nearest radio tower, allowing both Ukraine and Russia to track the movements of enemy forces. In this case, the Ukrainian side has an advantage because it owns the domain in which this radio traffic takes place and has the means to evaluate them<sup>14</sup>.

But it would also be important to mention in which area of warfare Russia was successful, at least initially. Namely in the field of electronic warfare. The Organization for Security and Co-operation in Europe (OSCE), observed and reported at the end of 2020 already, that there was a massive increase in the deployment of electronic warfare systems into the Russian-occupied Donbass. It took a few weeks until around

References  
on page  
39





mid-March 2022 for the Russian army to complete this marching up and begin to very successfully disrupt the exertion of Ukrainian drones. Especially at the beginning of the war, the Ukraine hoped that these drones would give them an advantage in reconnaissance, so that they could use their own artillery more successfully against Russia's much larger arsenal<sup>15</sup>.

Most recently, NATO has supplied Ukraine's armed forces with anti-drone jammers. The jammers are part of a comprehensive support package, said Secretary General Jens Stoltenberg on November 25th at a press conference in Brussels. In particular, the jammers are intended to help Ukraine fend off attacks with kamikaze drones. The devices are usually electromagnetic transmitters that interfere with the drones' navigation or communication systems but could also be used for interfering the Russian tank and/or artillery command and control systems<sup>16</sup>.

## THE INFORMATION DOMINANCE

Vladimir Putin's information space army of trolls, cybercriminals and warriors has shown the western world their destructive power for years. Their cyberattacks have interfered in countless elections and referendums, with Brexit and the 2016 US elections being the best-known examples<sup>17</sup>. They hacked western computer systems, spreaded viruses like NotPetya (one of the most disruptive cyberattacks in history) in Ukraine in 2017 and attacked western critical infrastructures like SolarWinds 2020 or Colonial Pipeline 2021. But they also fed conspiracy theorists and right-wing hardliners if you look at the stories about Q-Anon or western coronavirus vaccines<sup>18</sup>.

However, when the time came to oversee Putin's most ambitious and probably most important operation, the information space army appeared to have failed on all fronts. The goal has been to spread false information and tries to manipulate society, to push for actions that can destabilise the country during the war. But rather than the narrative of Russia as the Eastern leader fighting Nazis in Ukraine and protecting all ethnic Russians in the minds of Europe, Ukraine dominates so far, this online battle for the hearts of Westerners. And now it is very hard for Russia to change the narrative.

Nevertheless, the impression that Ukraine is clearly winning the "information war" is only true for Western observers. In social media in some African states, India, Pakistan or China, Russian disinformation actors are sometimes more successful in placing their narratives and memetic communication artifacts<sup>19</sup>. Russian propaganda can fall on fertile ground there because it also draws from negative cultural experiences in these countries. The fact that such an approach can then turn into the opposite was shown in September 2022 at the summit of the Shanghai Cooperation Organization (SCO) in Samarkand, where

many of the region's countries now look at China, not Russia, as the helping hand and development assistance<sup>20</sup>.

However, after many years of a far disproportionate dominance of Russian and European right-wing extremist propaganda - the two can often hardly be distinguished - the tide has turned mostly, especially on social media like Facebook, Twitter, and Instagram. Since the outbreak of the war, attempts have been made there, to circulate conspiracy narratives justifying the Russian invasion. The most common of these were that Putin had to invade to dig up secret bio-labs in Ukraine, where even more secret chemical and biological warfare agents were being produced on behalf of the CIA<sup>21</sup>. All of this seems somewhat spasmodic, and the spread of such fake news is more than limited and not successful.

The Russian Duma, meanwhile, passed a law providing prison of up to 15 years for publishing "false information" about Russian state operations. The law, passed by the Moscow Duma in its third reading, sets prison terms and fines for people who "knowingly spread false information" about actions by Russian government agencies "outside Russian territory"<sup>22</sup>.

Russian dis- and misinformation campaigns and attacks have come back at a high level. The floated fake news on the European population from September 2022 to denigrate the neighbours to the police if they heat their apartment to over 19 degrees was unsuccessful, because nobody believed that "news" and governmental authorities reacted immediately on social media<sup>23</sup>. Also, the recently launched disinformation campaign with Minister of Defence Shoigu as front man, who after a six-month break called his counterparts in the US, UK and France accusing Kyiv of wanting to detonate a radioactive, "dirty" bomb without presenting any kind of evidence, also failed because the US, France and the UK called the claim about a "dirty bomb" clearly false. A joint statement by the foreign ministers of these countries said "As a reminder, Ukraine does not have nuclear weapons! The world would see through any attempt to use this claim as a pretext for escalation"<sup>24</sup>.

## THE CYBERSPACE

The war in the cyberspace has begun long before the first Russian troops crossed the border into Ukraine. Since 2014 Ukraine has registered more than 5,000 cyberattacks on state institutions and critical infrastructure<sup>25</sup>.

By mid-2021, the hackers started to target digital service providers, logistics providers and supply chains in Ukraine and abroad to gain further access not only to Ukrainian systems but also to those of NATO member states. When in early 2022 all diplomatic efforts to de-escalate the conflict failed and the Russian military

began to complete its troop deployment along the border with Ukraine, cyberattacks rapidly intensified. The hackers were also increasingly using wiper malware, which erases hard drives and data, against Ukrainian institutions<sup>26</sup>.

Shortly after the invasion, websites of banks and government departments were attacked again in a next wave of attacks. At the same time, thousands of broadband users in Europe lost their Internet connection in a targeted attack on modems operated by the American satellite operator Viasat. The common goal of all these attacks was to shut down the command-and-control-systems of the Ukrainian officials and especially from the military<sup>27</sup>.

Principally, the Ukraine has expanded and improved its capabilities in the last years. With support from some western nations, like e.g., US, Israel, Lithuania, Netherlands, Poland, Estonia, Romania, and Croatia, which send cybersecurity experts to help Ukraine dealing with cyber threats<sup>28</sup>.

But Ukraine did not get only support from nations:

- The Anonymous collective immediately to support after the physical invasion. Starting with YourAnonNews, one mighty Anon account after another, which had been known for years, popped up on Twitter almost every day<sup>29</sup>. As a starting present, the website of the Russian Ministry of Defence was hacked and data records that were hidden on the server were published, while the notorious “Killnet gang” pledged support for Moscow and threatened retaliation.
- Anonymous posted on Twitter on May 21 that “the collective is officially in cyberwar against Killnet”. Shortly after Anonymous declared cyberwar, another message was posted saying that Killnet’s website had been shot down.
- So far, around 45 hacker groups have become active for the Ukraine. Most of them are loosely associated with Anonymous. All groups are running ransomware, psyops, hack and leak, DDoS, and defacement campaigns against Moscow<sup>30</sup>.
- Ukraine’s Minister of Digital Transformation, Mykhailo Federov founded in late February 2022 the Ukrainian volunteer “IT-Army” operating on Telegram. Currently around 300.000 volunteer hacker from all over the world are supporting the Ukraine by attacking Russian media, broadcasting, companies, etc<sup>31</sup>.

At all, Russia wanted to bring down Ukraine to its knees also in cyberspace. Russian attacks did some damage, but nothing dramatic so far. DDoS attacks, in which European and US websites are deliberately overloaded with data traffic and thus become unusable, cyber vandalism, in which websites are hijacked and redesigned can be observed as well<sup>32</sup>. Some of them were also coordinated with kinetic attacks, such as attacks on cellphone providers in regions that were simultaneously being shelled by Russian artillery or more previously by attacks against the critical infrastructure<sup>33</sup>. But nothing has hurt Ukraine so much right now that it couldn’t stay online. Russian hackers also managed successful attacks outside of the Ukraine. Noteworthy here are those attacks on government servers in Lithuania (May), Italy (June), Montenegro (August), Germany (September), Bulgaria and Poland (both in October)<sup>34</sup>. But none of them not repairable.

The fact that the Russian elite hackers with catchy names like “Fancy Bear”, “Snake”, “Sandworm” or “Killnet” have so far been able to cause relatively little damage only has even more reasons than Ukraine being well prepared for these attacks. Many experts observed the Russian attacks and made a devastating verdict. “Except for the satellite hack at the beginning of the war, all attacks were purely opportunistic. Nothing was thought out or well planned.” It seems, that the Russian online war is executed and fought like that on the ground: With brute force instead with finesse<sup>35</sup>.

#### **WHY IS THE RUSSIAN “CYBER- AND/OR INFORMATION PEARL HARBOR” STILL MISSING?**

One of the biggest surprises of the war so far is the absence of a visible, full-scale cyberwar, - also in information space. Why has the IT superpower Russia not yet mobilised all its cyber and information warfare potential in the war against the Ukraine? Why does “Cyber Armageddon<sup>36</sup>”, or “Cyber Pearl Harbor”<sup>37</sup> not happen so far? From the authors perspective, there are three explanations possible<sup>38</sup>:

##### Time- Hypothesis:

To cause greater damage, attackers would have to wait in the well-protected networks of Western companies and authorities to detonate their “virtual bombs”. However, even powerful, and well-trained cyber armies of western states would need at least a year to prepare such programs and would also be spy able against during that time. Russia’s hackers may have had much less time. Thus, the cyber and information warriors no longer found the necessary attention and support from the Kremlin

**References  
on page  
39**





because the military build-up in the other domains (land, sea, and air) needed all of Russia's power.

#### Preparedness- Hypothesis:

Kyiv may have learned the lessons of 2014 and is better prepared, as described also because of the help from western states and non-state actors. E.g., Microsoft is also helping the Ukraine by taking over Internet domains from the Russian hacker group Strontium (affiliated to Killnet) and redirected attacks into so-called "sinkholes"<sup>39</sup>. That would presuppose that the Western world was also better prepared for the Russian cyber and information war machine.

#### Uncertainty- Hypothesis:

That solution would be the most unpleasant and dangerous. Cyber Armageddon is not missing, - the Russian cyber and information warriors had enough time and support from Moscow to prepare a large-scale attack and implemented the virus already in our networks. But we don't know about it and Putin is just waiting to trigger it.

But no matter which hypothesis' might be the correct one, the lessons from Ukraine call for a coordinated and comprehensive strategy from EU and NATO to strengthen defenses against the full range of cyber -destructive, -espionage, and -influence operations.

### CONCLUSIONS AND RECOMMENDATIONS

Since the annexation of Crimea in 2014, it was believed that Russia had created a new form of modern warfare. Without firing a single shot, Putin's troops took control of the Ukrainian peninsula, which was considered the new gold standard for warfare through hybrid warfare especially with cyber means - a war in which tanks are not the focus, but instead disinformation, cyberattacks, sabotage, and special forces. No one in NATO and/or EU had believed Moscow would be capable of such an operation, everyone had been taken by surprise. But it is now apparent that the Russians are not as far along as assumed. The underestimation of the Ukrainian public will to resist led to the fact that the



**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**

hybrid attack on Ukraine become a hybrid war which went rogue, and which is now also a conventional war.

However, also in this war, the cyber and information space, using the electromagnetic spectrum is still one of the most important parts of the battlefield, it's not just only about pure propaganda.

What should NATO and the EU expect in the future and what could be done?

The West is likely to be prepared for a protracted, mostly low-intensity war. Putin already perceives the imposition of sanctions almost as a declaration of war. For Russia, the tool of retaliation could be cyber and disinformation operations. In its report from June 2023 Microsoft warned of an increase of Russian military offensive cyber operations (wiper malware) against European critical infrastructures<sup>40</sup> in the next months. But also cyberattacks from actors like "Cadet Blizzard" they are associated with the Russian GRU. These attacks, which began in February 2023, targeted government agencies and IT service providers in Ukraine. Collective Western efforts towards cyber resilience, both at national, EU and NATO level, therefore, urgently need to be stepped up.

The cyber threat landscape is evolving at a rapid pace. Europe and the US must now prepare for ongoing gray area conflicts. Only through anticipation, risk mitigation, and creativity can they shift the balance of power in cyberspace in favor of the defenders of a whole, safe, and free Internet.

EU and NATO countries should develop satellite capabilities to provide coverage and connectivity to the global internet. This would become part of a global doctrine to encourage open information provided in conflict zones and authoritarian internet shutdowns. The logic should follow that of Cold War shortwave radio.

Whoever wins inside cyberspace decides what people and societies believe and what they think truth looks like but also, what is happening physically on the ground. Because whoever loses the battle for information also loses the moment to act and win the physical war. It currently looks, that Russia is not in favor to win that war, - not even in information- and cyberspace. ■



**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. Similar articles and its content has been published by the author already in several magazines in 2023 (TDHJ, ÖMZ, Hybrid CoE flash findings, CyberWatch Magazine, etc.). This essay is a continuation of the events in the Ukraine war.
2. See also: Angela Stent: "Putin's World : Russia Against the West and with the Rest", 2020, Twelve, US, p12-25
3. Like described from James O. Finckenauer and Yuri A.Voronin in "The Threat of Russian Organized Crime", NCJ 187085 from June 2001
4. <https://www.c4isrnet.com/cyber/2021/03/25/us-military-conducted-2-dozen-cyber-operations-to-head-off-2020-election-meddling/> (Unless otherwise indicated, all links were last accessed on 08.01.2022)
5. <https://www.watson.ch/international/russland/444993013-nachrichtenagentur-des-kremls-ruft-zur-vernichtung-der-ukraine-auf>
6. according to the task force of the European External Action Service "EUvsDisInfo", <https://euvsdisinfo.eu/report/russia-fights-the-collective-west-not-just-ukraine>
7. The author understands "Narratives" as overall messages that are spread and constantly repeated in the form of individual texts, images and videos by fake accounts in social networks or on supposed news portals. Individual reports always contribute to a message, a narrative. Some of these narratives have been used for many years, combined or altered according to current events and settings.
8. <https://www.cyberscoop.com/russia-ukraine-cyberwar-nato-geneva-microsoft/>
9. Germany f.e. sees it together (<https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum>). GB and the the US not (<https://www.cybercom.mil/>, <https://www.ncsc.gov.uk/>)
10. Therefore I mostly agree with Stefan Libicki's essay from 1995: "Is there an elephant? Seven forms in search of a function: Command-and-control warfare, Intelligence-based warfare, Electronic warfare, Psychological warfare, Hacker warfare, Information warfare, Cyberwarfare" (<https://apps.dtic.mil/sti/pdfs/ADA367662.pdf>)
11. See also Nicolas Mazzucchi "AI-based technologies in hybrid conflict: The future of influence operations", Hybrid CoE Paper 14, June 2022.
12. <https://www.nzz.ch/international/der-elektronische-krieg-in-der-ukraine-unsichtbar-aber-wichtig-id.1688611?>
13. <https://kurier.at/politik/ausland/elon-musk-ukraine-russland-putin/402186138>
14. <https://www.newscientist.com/article/2315553-russia-and-ukraine-are-both-weaponising-mobile-phones-to-track-troops/>
15. <https://www.forbes.com/sites/davidaxe/2022/12/24/russia-electronic-warfare-troops-knocked-out-90-percent-of-ukraines-drones/>
16. <https://orf.at/stories/3295244/> The Russian army has been increasingly attacking ukrainian critical infrastructure with kamikaze drones since October 2022, using mainly Iranian-made aircraft Shahed-136. It has a triangular wing and is equipped with a warhead. The drone is usually launched from trucks and crashes towards its target at high speed, but can be interfered by electromagnetic attacks.
17. <https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections>
18. <https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/>
19. <https://carnegieendowment.org/sada/87353>
20. <https://www.politico.eu/article/russia-disinformation-africa-europe-sergey-lavrov/>
21. <https://www.bbc.com/news/60711705>
22. <https://www.independent.co.uk/news/world/europe/ukraine-war-latest-russia-law-b2028440.html>
23. Neue Zürcher Zeitung (intern. Edt.), Donnerstag 15.September 2022, p6
24. <https://orf.at/stories/3291109/>
25. <https://www.databreaches.net/security-service-of-ukraine-identified-fsb-hackers-who-carried-out-more-than-5000-cyberattacks-on-state-bodies-of-ukraine/>
26. <https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat>
27. SonntagsZeitung, Samstag 9 April 2022, S. 17
28. <https://carnegieendowment.org/2022/06/16/ukraine-war-shows-how-nature-of-power-is-changing-pub-87339>
29. The largest accounts have over 15 million followers: (<https://www.derstandard.at/story/2000134361378/anonymous-sind-zurueck-wie-der-cyberkrieg-gegen-russland-ablaeuft>)
30. <https://orf.at/stories/3256364/>
31. <https://t.me/itarmyofukraine2022>
32. <https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/>
33. <https://www.ohchr.org/en/press-briefing-notes/2022/10/ukraine-attack-civilians-and-infrastructure>
34. <https://orf.at/stories/3284892/> as well as <https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland>
35. See the interview with Marina Krotofil: <https://securityboulevard.com/2022/08/bsidestlv-2022-marina-krotofil-kinetic-and-cyberwarfare-twins-siblings-or-distant-relatives-or-why-bombs-speak-louder-than-electronic-bits/>
36. Or cyber apocalypse? Implies that critical infrastructure within one or more countries is continuously bombarded with ransomware and other attacks so that every civilian service is either dramatically slowed or shut down.
37. The term was coined in 2012 by U.S. Defense Secretary Leon E. Panetta and aims to relate the intensity and potential devastation of a major cyber-attack with the 1941 attack on Pearl Harbor, a surprise military attack by the Japanese Navy against the U.S.
38. Thank You Stephanie Carvin for sharing Your article: "How to Explain the Failure of Russia's Information Operations in Ukraine?" from March 2022 (<https://www.cigionline.org/articles/how-to-explain-the-failure-of-russias-information-operations-in-ukraine/>). Your thoughts inspired me for that conclusion.
39. <https://www.csoonline.com/de/a/microsoft-uebernimmt-domains-von-russischen-hackern,3673868>
40. <https://blogs.microsoft.com/on-the-issues/2023/06/14/russian-cyberattacks-ukraine-cadet-blizzard/>



# MONTHLY REVIEW

## OCTOBER 2023

// Cyberwatch Finland Analyst Team

### CONTENT:

#### 1. EVENTS IN THE CYBERLANDSCAPE

- 1.1 International Cyber Environment
- 1.2 Cybercrime
- 1.3 Technology

#### 2. IN THE SPOTLIGHT

- 2.1 Traditional Crime is Easier to Carry Out in the Cyber Dimension
- 2.2 International Cyber Cooperation has Positive Potential

#### 3. FOLLOW THESE

- 3.1 France's Direction Remains Unclear
- 3.2 Security Authorities More Frequently Targets of Cyber Influence
- 3.3 What Happened to Ukrainian Cybercrime?

#### REFERENCES

ATTACHMENT 1 Threat Intelligence Review





## IN THE MONTHLY REVIEW

Regarding to the international cyber environment, the speech of the President of the EU Commission, Ursula von der Leyen, on the role of the EU in promoting digitalisation through, among other things, the development of regulation, was highlighted in September. The conflict in the Nagorno-Karabakh region was also presented from the point of view of cyber operations, as their role has become increasingly central in the toolbox of both parties of the conflict. The International Criminal Court (ICC) also announced in September that it will start investigating crimes made in the cyber environment as war crimes.

About cybercrime, the future goals of the UN conference on cybercrime for the development of an even better global cybercrime regulation were on the surface. In addition to this, there was an increase in the reporting of technological disruptions as cyberattacks, without more precise grounds, which indicates a change in interpretation methods and the social fear created by the cyber threat. With the development of technological devices and applications, advanced and freely available data recovery tools emerged for victims of ransomware. In addition, in terms of technology, the development of Web3 technologies and the impact of the downturn on IT and cybersecurity organisations also raise concerns.

In the review, we look at the main topics of the

previous month, tying them into a wider context. Our review is divided into three perspectives: continuous monitored phenomena, from which we select the most significant to be addressed; phenomena that we want to highlight especially from the previous month and phenomena which development is worth following. A threat intelligence report on the month's most significant cyberattacks and active threat actors is submitted as an attachment to the monthly review.

In this review, we discuss how crimes familiar from the traditional world are being adopted more rapidly in the cyber environment, and how the physical world and the cyber dimension are becoming more closely intertwined. In addition to this, we examine how international cooperation in the cyber environment has developed over the past few months and what positive outcomes cooperation can result despite the significant challenges. It is especially worth following from the events of September to see in which direction France's approach to monitoring social media and the internet is developing. Another important phenomenon to monitor is how the security authorities are increasingly the targets of cyberattacks. The most recent examples have been cyberattacks against police force in Great Britain. It is also worth considering whether Ukrainian cybercrime has stopped since the start of the war in Ukraine. ➤





## 1. EVENTS IN THE CYBERLANDSCAPE

### 1.1. International Cyber Environment

Political speeches, international conflicts and the International Criminal Court have been on the surface recently. The most interesting political outcome of the month was the State of the Union address given by President of the European Commission Ursula von der Leyen, which is one of the most followed political speeches in the world. The speech is given once a year and it defines the Union's future guidelines, tells about the Union's will and recounts the past from the EU's perspective. This year's speech devoted its share to digitalisation and artificial intelligence. The speech reflected the EU's ambition to be a pioneer in the digital environment. Von der Leyen highlighted the EU's pioneering role in citizens' digital rights and praised how EU regulation makes the digital environment safer. Artificial intelligence and the threats and opportunities it brings were also mentioned. Although the themes were often approached from a regulatory perspective, the speech can be interpreted as part of the EU's broader goal towards digital sovereignty. Digital and AI issues are currently on the surface, and the Union has a vocal desire to promote them also in the future. This is important if the EU is to be able to maintain its position in a changing world in the midst of great powers such as China and the United States.

The crisis that flared up again in Nagorno-Karabakh on 19 September is also significant from a cyber perspec-

tive. The conflict is between Armenia and Azerbaijan and was followed by an immediate increase in the number of cyberattacks in both countries. The conflict has already smouldered in the online dimension, as cyberattacks have been seen on both sides over the years. Governments have also had access to the most advanced cyber tools – Amnesty International, for example, has pointed out the use of Pegasus and Predator spyware in both countries. The crisis shows once again that the cyber dimension plays a role in different types of conflicts.

In September, the International Criminal Court (ICC) announced that it would start looking at crimes in cyberspace as potential war crimes. This would be based on the so-called Rome Statute, according to which the Court has the right to investigate and judge war crimes, crimes against humanity and crimes related to genocide. However, it is unclear how state-sponsored cyberattacks fit into this framework, or how states can be shown to be behind them. Often, states use criminal hacker gangs as their covers or are always able to camouflage and deny their activities. However, the announcement is a step in the right direction and signals that the cyber environment is also being taken seriously and criminals are being held accountable. The ICC itself has not escaped cyberattacks either, as in September it was also the victim of a cyberattack itself. However, the attack is not necessarily related to this particular report, but may be due to, for example, other ongoing investigations by the court.

# CYBER CRIME CYBER CRIME

## 1.2. Cybercrime

In September, some of the most significant cybercrime-related events included UN and ICC efforts to combat cybercriminals and cyberwar criminals, on the one hand, and news of increasingly diverse and evolving forms of cybercrime on the other. At the beginning of September, the UN concluded its fifth working group conference on cybercrime legislation, with the aim of producing a working paper early next year that could serve as a basis for future global cybercrime legislation. Also in September, the Chief Prosecutor of the International Criminal Court announced objectives to start investigating and prosecuting war crimes in cyberspace. Both events tell the same story of how cyber operations challenge existing legislation and are quite difficult to deal with within the framework of current regulations. Cybercrime is almost always international in nature, and identifying the perpetrator and, in particular, proving guilt are significant challenges even in situations where the perpetrator and victim would be subject to the same legislation. The current regulatory field is largely incapable of responding to this problem, and while it is good that work is being done to harmonise laws at the global level, there is still a long way to go and many challenges ahead.

The phenomena related to cybercrime itself highlighted the ways in which the cyber environment continues to play an increasingly important role in crimes that do not really fit the "pure" definition of the phenomenon. In practice, these are crimes in which the cyber environment plays some part in the operation, but do not occur exclusively in the cyber environment, but break the line between the physical world and cybercrimes. These may be small-scale crimes, where digital devices support more traditional forms of crime, or, on the other hand, the activities of large-scale international criminal organisa-

tions, which, for example, combine deprivation of liberty with cybercrime. The boundaries between these two crime worlds, which have long been seen as separate from each other, seem to be blurring, as the possibilities for action increase and at the same time the benefits become more tangible. These developments will be discussed in more detail later in this review.

Not only is cybercrime evolving, but it also seems that attitudes towards it have changed considerably in the last few months alone. In addition to the work done solely for law enforcement, this is evidenced by the ever-increasing attention paid by the authorities, the focus of politics on the cyber world, the seriousness of the crimes committed, and the level of fear aroused by cyber threats. For many, the cyber environment still feels like an unfamiliar field of activity and a somewhat unknown threat. The news about devastating cyberattacks from around the world has caused a phenomenon where, in any disruption or outage, the first suspicion and worst fear is being the victim of a cyberattack. Because communicating about these is also important, there have recently been several examples of cases where a party experiencing a technical incident has even reported having been the victim of a cyberattack before the real cause of the fault has been determined. However, in order to avoid fearmongering and to maintain one's own public image, it is important to first ascertain the nature of the event before external communications. While it is good that cyberattacks are taken seriously and that the communication related to them is open and fast, care should be taken to make sure that this communication is also correct and factual. Rushing to conclusions should be avoided so that the extent and nature of the damage can be accurately assessed, and follow-up measures should be scaled accordingly.

References  
on page  
50







### 1.3. Technology

In terms of the technological situation, there was good news in September about the tools and solutions available to those affected by cyber threats. Namely the news came in the form of free-of-charge data recovery tools developed for ransomware victims, both quantity and quality of which have increased significantly recently. There are openly available completely free tools online that can recover files encrypted by a variety of ransomware. During September, this already extensive range of tools was added to when a python script was released for countering malware used by the Key Group hacker group. With this script, it is possible to decrypt and restore the original filenames encrypted by the malware. This is rare news because more often we come across new technological methods used by criminals in their activities than solutions to respond to the threat or limit the damage suffered by victims. Despite the positive news, it must be borne in mind that criminals have already partially shaped their activities with this development in mind. Extortion attacks are less and less dependent solely on the security of data encryption, but often also threatening data leakage outwards or its open publication, for example.

When it comes to technical cyber protection, we should not forget the most important measure, which is to update systems properly. In September, this demand was again highlighted when news broke about the ever-increasing speed at which criminals exploit vulnerabilities that they have detected themselves or that have been published openly. Similarly, the importance of updating systems was also highlighted when news broke about popular and effective forms of attacks, such as web skimming, which are entirely based on poorly protected systems. Although this is not a new technological situation where installing security updates and being aware of

vulnerabilities in one's own systems is critical, the same advice cannot be repeated too much.

In terms of the future, in September, both the potentially growing role of Web3 technologies and the potential impact of the downturn and recession on the financing of the IT and cybersecurity sector were discussed. Web3 and related technologies have been on the surface for a long time, and those who swear by them have been waiting and predicting a radical overhaul of the entire internet-based infrastructure. However, this does not seem likely in the near future. Even though blockchains or certificate systems based on them are constantly evolving and finding new uses, it is possible that the concept of Web3 as a new era of the internet will remain a vision for the future. However, many companies using and marketing these technologies have found some funding, which in today's economic climate is no longer nearly as self-evident as it might be for companies focusing on information technologies. In particular, the exponential growth in the number of cybersecurity providers has led to the fact that, although the issue is becoming increasingly important and receiving more attention, there is simply no niche for all new players. Winning the competition for projects is becoming increasingly difficult, and there is a risk that, as in so many other fields business, the big players will ride roughshod over the smaller ones, stifling innovation and reducing the number of options available to consumers.



## 2. IN THE SPOTLIGHT

### 2.1. Traditional Crime is Easier to Carry Out in the Cyber Dimension

Crimes familiar from the traditional world are quickly adopted in the cyber environment, where technology acts as a means of committing the crime or in some form as a mediator of the crime. In the past, crimes against people and individuals have now, thanks to technology, become even more diverse and become easier to execute. Cyber-crime and traditional crime are becoming more connected, and it is becoming quite difficult to distinguish them from each other. For example, scams based on digital platforms are just one form of activity among other criminal activities. Cybercrimes have long been thought to be committed only by criminals who has specialised in them, but now it is easy to carry out cybercrimes without the criminal having any special technical skills.

One example of this is the combination of human trafficking and cybercrimes. According to a UN report, reports of human trafficking related to cybercrimes have constantly increased. In cases of human trafficking, the victim is violently deprived of freedom, the ability to keep in touch with home and loved ones, and the victims are ultimately forced to commit cybercrimes in the name of their oppressor without them themselves benefiting from the crime in any way. Most often, cybercrimes that take advantage of victims of human trafficking are crypto or romance scams of various levels, but frauds related to gambling have also become more common. The party committing the fraud does not necessarily need to know

anything other than to produce messages that sound believable, as the fraud websites and tools used for crimes are now sophisticated, easy to use and highly automated. This type of activity is on the rise, especially in Southeast Asia, and it is not the only form of activity or source of income for the criminal organisations that practice it, but one method of committing a crime among others. It is therefore good to understand that cybercriminals are not automatically always evildoers, but the perpetrator of a cybercrime may also be the victim of a crime.

Another example of the cyber dimension becoming part of the problems of the physical world is the new dimension of domestic abuse, digital domestic abuse. Digital domestic abuse refers to technology-enabled harassment, bullying, intimidation or stalking of loved ones. It can happen for long periods of time, and it usually only gets worse over time. Digital domestic abuse can manifest itself as, for example, going through the page history of partner's web browser, unauthorised reading of emails, monitoring and controlling the activities in social media, sharing intimate photos without permission, regularly reviewing the contents of the phone, demanding usernames, and passwords, or even installing spying devices or locators on a loved one's belongings or smart devices. With the development of technology and social media platforms, this kind of controlling and harassment has become increasingly easier to implement. Where social media services have offered individuals even better ways of interacting, they have also increased some individuals' sense of insecurity in an already challenging life situation.

References  
on page  
50







## 2.2. International Cyber Cooperation has Positive Potential

Cooperation in the cyber world has been somewhat on the agenda in September. Whether it is a question of harmonising legislation or cooperation between authorities in different countries and private security companies, it is clear that international cooperation in cybersecurity is a concrete way to respond to cyber threats on a global level. As has been said many times, there are still many challenges with these processes, and these are not small issues that can simply be shrugged off. However, it is also good to keep in mind the potential benefits that developing cooperation can have.

In addition to the low risk of being caught, one of the factors that most affects the popularity of cybercrime is the very low probability of actually being held accountable. This is due not only to the challenges of finding evidence, but also to the fact that crimes are often committed from the other side of the world than where the victims are located. Due to these factors, the investigation of cybercrime requires considerable technological competence and the ability to invest resources in solving cases, as well as international cooperation between authorities to carry out arrests and confiscate the proceeds of crime. Although there are many discussions about how difficult it is to achieve this in practice, there are more and more examples of successful cases. In these cases, the authorities of different countries, often in cooperation with a private cybersecurity company, have investigated criminal cases, leading to arrests, closure of illegal services and confiscation of assets. Typically, in this equation, private security actors have provided forensics capabilities, and cooperation between authorities has been coordinated by Interpol or another global organisation.

Private companies often have the opportunity to analyse first-hand data from victims' systems through their customers, and it is an excellent advertisement for services if they can address international cybercrime.

Recent examples of successful operations by the authorities are many. One such is the operation led by Interpol and Afropol, where, thanks to cooperation between the authorities of more than 25 African countries, 14 people were arrested and more than 20,000 online services were shut down. In another example operation, 16shop - a platform offering phishing tools based in Southeast Asia was shut down. In this case private companies such as Groub-IB, Palo Alto and Trend Micro played a significant role in addition to Interpol. An even more recent example that affects Finns more closely is the closure of the Piilopuoti website focusing on drug sales from the Tor network by Finnish Customs in September. In addition to the Finnish authorities, police forces from both Germany and Lithuania were involved.

Cooperation in the cyber world is therefore possible and can also achieve results in responding to cybercrime. However, too much hope should not be placed on the processes aimed at promoting UN cyber legislation, for example, but it is good to remember that cooperation is constantly evolving. In addition, the abilities of both public authorities and private actors to respond to the threat posed by cybercrime is constantly advancing. Although it is unlikely that we will never, or at least not in the near future, get all the countries of the world around the same table to genuinely negotiate on curbing cybercrime, even small advances are still valuable.





### 3. FOLLOW THESE

#### 3.1. France's Direction Remains Unclear

France's direction in terms of internal and online control has been a hot topic in Europe throughout the year. The AI surveillance law in the spring and President Macron's comments this summer on social media moderation raised widespread opposition and concern not only internally but also across Europe about France's direction towards a surveillance society. Among other things, citizens' right to privacy and a free internet has been seen at stake. With the autumn rains, it has been revealed that criticism and opposition have not affected the government's policy.

Recent developments include a fast-track French law that would force web browser developers to block access to certain government-sanctioned websites. Critics say this could lead to online censorship, and web browser giant Mozilla has begun collecting names for a petition to stop the bill. As a giant of the European Union, France's development can also set the course in Europe and set an example for censorship in authoritarian states around the world. The online environment seems to be on the surface in the country anyway, as major newspapers in the country, for example, announced that they had blocked

Open AI's GPTBot data collection from their own websites. This is mainly due to business reasons, such as the reluctance to distribute the produced content free of charge to a party from whom nothing is received in return. In addition, the reluctance to be associated with false and inaccurate content generated by artificial intelligence was cited as a reason.

France's plans to ban iPhone 12 sales also received extensive international coverage. In this case, there was no actual cybersecurity aspect, although Apple has recently been in the news due to critical vulnerabilities in its software, which have since been fixed. On the other hand, concerns have been raised about electromagnetic radiation emitted by the devices, which would exceed the limit values. However, the authorities' intention to ban the sale of the device has something in common with the bill on censorship of web browsers. At the end of the day, it all boils down to the difficult distinction between the rights and obligations of individuals and businesses and the protection imposed or provided by the state. Even if the arguments behind France's actions are seen as creating a safer online environment, the measures can easily go against the original idea.

References  
on page  
50







### 3.2. Security Authorities More Frequently Targets of Cyber Influence

In August, it was reported how the police authorities in Great Britain had become the target of a cyberattack. In the attack, the subcontractor of Greater London's policing was target of a data breach, which resulted the names, photos and, for example, information about the positions of individuals in the police force, were leaked on dark web. At worst, the leak affected all 47,000 staff members working in the police department, and affects, for example, the safety of undercover officers. Now in September, the Manchester area police authority announced that it had been the target of a ransomware attack, in which it had also lost the officers' personal information and ID numbers. There is less than a month between these two attacks, and they also had in common the fact that the attacks were carried out by exploiting a subcontractor of the police authority.

In addition to these, in July, just a few months before the cyberattacks on Great Britain, the police of Northern Ireland inadvertently suffered a data leak, in which the data of more than 10,000 of its officers and staff leaked online. Especially in Northern Ireland, the situation is still very vulnerable due to the long-standing ethnic conflicts, which has been reflected especially in the need for the police to protect their privacy even more closely. In the case, the police authority had responded by email to a request for information, to which a table relating to the personal information of the authorities and staff was inadvertently linked. In addition to this case, documents were also stolen from the Northern Ireland police force in another data leak, which contained, among other things, the information of police officers working in the field. The information from both data leaks later ended up on

the dark web, and the Northern Ireland police have considered, for example, the role of the Irish Republican Army (IRA) in both incidents.

In addition to these, North Korea has been reported to have targeted cyberattacks against, for example, a Russian missile manufacturer in recent months. Now, the latest report published by Microsoft in September states that this was by no means a unique attack from North Korea, but that it has targeted its attacks against the Russian administration, army, and defence technology several times since the beginning of the year. North Korean cybercriminals are also known to have extended their cyberattacks to German, Israeli, Brazilian, Czech, Italian, Norwegian, Polish, and Finnish defence industries. According to Microsoft's report, 5 percent of North Korea's espionage activity in the past year have targeted Finnish defence technology. China and Iran, along with North Korea, are known for currently focusing their state cyber operations especially on the authorities and defence technology of their neighbouring countries and the US administration.

The security authorities have indeed become a very interesting target for cyber influence, because an attack can easily cripple a significant social actor, but at the same time, the information gathered through these crimes is extremely valuable to many traditional crime actors, thus increasing the security threat both nationally and internationally. The disadvantages of cybercrimes against security authorities may soon materialise into an even worse real-world threat, especially for its victims. In particular, the safety of persons working in covert missions and secret operations can be very much threatened.



### 3.3. What Happened to Ukrainian Cybercrime?

Ukraine has previously been known for its sophisticated and high-level cybercrime. Before the war, it was seen as a problem plaguing the country, and NATO's Cyber Defence Centre of Excellence in Tallinn raised the issue in 2018 in a report describing Ukrainian cybercrime and considering whether Ukraine is a safe haven for cyber-criminals. There are many examples of successful Ukrainian hackers' work, and over time, hackers have managed to steal tens of millions of dollars of money, for example from US bank accounts. Ukraine has also been a favourable growth environment for cybercriminal activities due to its relatively low standard of living and wages, corruption and, on the other hand, high-quality IT education provided in higher education institutions.

However, since the war, relatively little has been said about Ukrainian cybercrime. The main focus has been on reviewing war-related cyber operations, their successes and failures. In particular, Russia's cyberattacks on Europe have been on the surface. Naturally, as sympathies are broadly on Ukraine's side, there may also have been a desire to keep quiet about the subject and problems and thus show support in Ukraine's fight against the invasion. However, cybercrime is unlikely to have disappeared from the country, although it has undoubtedly changed shape. For example, Google has reported the partial dispersal of cybercriminal gangs in Eastern Europe due to war and political opinions. In the past, it has been natural for Russians and Ukrainians, for example, to cooperate because of their common language and culture.

There have also been reports of successful arrests of cybercriminals throughout the year. A possible explanatory factor here may be the need to signal to Western

partners the effectiveness of operations and to show that, at least no longer, the country acts as a safe haven for crime. In the spring, the country's cybercrime police announced the arrest of a man who had sold personal data of Ukrainians to Russians. In the summer, Europol announced a cooperation operation between Germany and Ukraine, in which the perpetrators of the major Doppelpaymer ransomware were successfully arrested. Although arrests have been made and some cybercriminals have probably started to use their skills for good as a result of the war – for example, in the ranks of Ukraine's own IT army – cybercrime as a phenomenon certainly still lives under the surface. International aid money is constantly flowing into the country, donations are made through various online platforms and websites and, for example, in the form of cryptocurrencies. It would be extraordinary if at least part of this assistance did not also end up in the pockets of cybercriminals. For example, there have been reports of cases where phishing sites, promising support to Ukraine, have been used to scam victims out of money.

Recently, due to the slow progress of the Ukrainian counteroffensive, the military action and the situation have started to be discussed in the media in a more critical tone. Quick victories are no longer expected, and the activities of the armed forces and society have also been critically examined from the perspective of corruption, for example. It would be no wonder if, in the news about the cyber dimension of the war, Ukrainian cybercrime also made a comeback on the list of news topics.

**References  
on page  
50**





## REFERENCES

### INTERNATIONAL CYBER ENVIRONMENT:

Cyberwatch Finland 2023 Weekly Review, week 38  
Cyberwatch Finland 2023 Weekly Review, week 39  
[https://ec.europa.eu/commission/presscorner/detail/en/speech\\_23\\_4426](https://ec.europa.eu/commission/presscorner/detail/en/speech_23_4426)

### CYBERCRIME:

Cyberwatch Finland 2023 Weekly Review, week 36  
Cyberwatch Finland 2023 Weekly Review, week 37  
Cyberwatch Finland 2023 Weekly Review, week 38

### TECHNOLOGICAL DEVELOPMENT:

Cyberwatch Finland 2023 Weekly Review, week 36  
Cyberwatch Finland 2023 Weekly Review, week 37  
Cyberwatch Finland 2023 Weekly Review, week 38

### TRADITIONAL CRIME IS EASIER TO CARRY OUT IN THE CYBER DIMENSION:

Cyberwatch Finland 2023 Weekly Review, week 37  
Cyberwatch Finland 2023 Weekly Review, week 38

### INTERNATIONAL CYBER COOPERATION HAS POSITIVE POTENTIAL:

<https://www.interpol.int/News-and-Events/News/2023/Notorious-phishing-platform-shut-down-arrests-in-international-police-operation>  
<https://tulli.fi/-/tulli-takavarikoi-piilopuoti-kauppapaikan-verkkopalvelimen-jalleen-merkittava-onnistuminen-anonymissa-tor-verkossa>  
<https://www.interpol.int/News-and-Events/News/2023/Cybercrime-14-arrests-thousands-of-illicit-cyber-networks-disrupted-in-Africa-operation>

### FRANCE'S DIRECTION REMAINS UNCLEAR:

<https://www.reuters.com/technology/why-has-france-banned-sales-apples-iphone-12-2023-09-13/> <https://www.euractiv.com/section/artificial-intelligence/news/several-french-media-block-openai-gptbot-over-data-collection-concerns/>  
<https://foundation.mozilla.org/en/campaigns/sign-our-petition-to-stop-france-from-forcing-browsers-like-mozillas-firefox-to-censor-websites/>

### SECURITY AUTHORITIES MORE FREQUENTLY TARGETS OF CYBER INFLUENCE:

Cyberwatch Finland 2023 Monthly Review, September  
<https://www.securityweek.com/a-second-major-british-police-force-suffers-a-cyberattack-in-less-than-a-month/>  
<https://www.securityweek.com/northern-irelands-top-police-officer-apologizes-for-industrial-scale-data-breach/>  
<https://www.bleepingcomputer.com/news/security/microsoft-north-korean-hackers-target-russian-govt-defense-orgs/>  
<https://blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea/>

### WHAT HAPPENED TO UKRAINIAN CYBERCRIME?:

[https://www.ccdcoe.org/uploads/2018/10/Ch13\\_CyberWarinPerspective\\_Kostyuk.pdf](https://www.ccdcoe.org/uploads/2018/10/Ch13_CyberWarinPerspective_Kostyuk.pdf)  
<https://www.zdnet.com/article/the-war-in-ukraine-has-shaken-up-the-cybercriminal-ecosystem-google-says/> <https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets>  
<https://therecord.media/ukraine-arrests-man-for-selling-data-on-300-million-to-russians>





# THREAT INTELLIGENCE REVIEW

Cyberwatch Finland publishes the 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.

## MAJOR CYBERATTACKS AND CAMPAIGNS

### INTERNATIONAL CRIMINAL COURT, ICC

DATE: 19.9.2023

DESCRIPTION: International Criminal Court, the tribunal located in the Hague in the Netherlands, which is responsible for prosecuting war crimes declared having been subjected to a cyberattack. ICC has been in the news lately accusing several high-profile Russian politicians of violating international law. For example, an arrest warrant was issued for President Vladimir Putin in spring 2023. Relatively little is known about the cyberattack and its investigation is still ongoing. At worst, it is possible that some of the court's encrypted documents or information about ongoing investigations, for example, have been leaked to hackers.

ACTOR: No definite information, but suspicions were directed at Russia or one of the criminal coups it employs.

MOTIVE: Unclear, potential goals might have been theft of confidential documents or disruption of court operations, or a simple information influencing value by gained by attacking a high-profile target.

IMPACT: The court itself has not reported that any data has ended up in the hands of criminals or other adverse effects it has experienced. However, according to Dutch public broadcaster NOS, classified information had been leaked, which could have an impact on ongoing court investigations.



# MAJOR CYBERATTACKS AND CAMPAIGNS

## MOROCCAN EARTHQUAKE

DATE: September

DESCRIPTION: French-speaking cybercriminals developed a scam to trick people into donating money to help victims of the earthquake in Morocco. Cybercriminals register domains with which they tried to impersonate humanitarian aid organisations, such as the French Red Cross in this case. Often, after a disaster, humanitarian non-governmental organisations start collecting funds for the disaster areas. This, in turn, attracts online fraudsters to collect funds in the name of a disaster, just as they are currently collecting criminal monetary donations in the name of the earthquake in Morocco. Cybercriminals may also sell products on their fake websites to "raise funds" for disaster victims. In this case, the victim may lose not only the money but also their bank card information.

ACTOR: Not published

MOTIVE: Economical

IMPACT: The effects are greatest for those who donate through fake websites. In addition to money transfers, the victims may also lose their personal information and bank and credit card credentials. It also causes reputational damage for the organisations that the fake sites imitate.

## TRAFICOM

DATE: 18.09.2023 and 07.09.2023

DESCRIPTION: The Finnish Transport and Communications Agency Traficom was hit twice in September by a denial-of-service attack. The attacks are part of a wider wave of attacks on Finnish authorities and public administration targets, which are often carried out by pro-Russian hacker groups as a way to oppose decisions made by Finnish authorities or political decision-makers regarding Russia. According to its own reports, the same hacker group has also targeted for example Helsinki Central Station and a company arranging cruises on Lake Saimaa in September.

ACTOR: Russian hacker group NoName057(16). This group carries out low-level DDoS attacks on a daily basis against actors it perceives to be anti-Russian around the world.

MOTIVE: Information influencing and arousing fear in Finns.

IMPACT: Very minor. Some of Traficom's online services suffered from temporary malfunctions, but there was no long-term impact or any kind of data leak.

## MGM GROUP

DATE: 11.9.-19.9.2023

DESCRIPTION: MGM Resorts, a hotel and casino giant, was the victim of a large-scale cyberattack in September. The attack extensively affected the company's operations, and it was only nine days after the attack that the company announced that operations were fully restored. The company has also been a victim in the past, as in 2019 the data of more than 10 million customers leaked online.

ACTOR: The ransomware exploiting ALPHV (also known as BlackCat) hacker group claimed responsibility.

MOTIVE: Economical

IMPACT: The company's website, booking system, casino ATMs, slot machines and credit card machines were affected. At least 30 hotels and casinos owned by the company were affected.

# ACTIVE THREAT ACTORS

## SANDMAN

**DESCRIPTION:** A previously unknown threat actor whose country of origin or size is unknown. The modus operandi has been described as advanced and has been defined in several sources as an APT group-ing, suggesting state activity in the background.

**RECENT ACTIVITY:** Telecommunications companies operating in the Middle East, Western Europe and South Asia have been particularly targeted.

**METHODS AND TACTICS:** Exploits infostealer malware named LuaDream that steals data from the user's device. Information obtained through espionage can be used, for example, to plan new cyberattacks, the information can be used to blackmail the target, or the information can be sold on dark web marketplaces, if necessary. The information itself can also be valuable to the attacker.

## CACTUS RANSOMWARE

**DESCRIPTION:** Active since March 2023. Targets its attacks on large commercial sectors, the financial sector and the construction sector. The group uses typical ransomware tactics, but as its own specialty, it has an additional anti-tracking feature. So far, the origins of the group have not been made public.

**RECENT ACTIVITY:** The group is known to have recently added five high-profile victims to its forum on Dark Web. The victims are from different parts of the world and represent different industries. The large companies in the last listing are mainly from the United States, Canada or, for example, France.

**METHODS AND TACTICS:** In particular, the group exploits identified VPN vulnerabilities to gain access to target systems. Uses many different tactics, techniques and procedures in its ransomware attacks. In addition to ransomware attacks, the group also steals data from its victims.

## BIANLIAN

**DESCRIPTION:** Originally detected as early as 2019, in 2022 resurfaced now as BianLian ransomware. There is no exact information about the group's home country, but it is known especially for blackmail attacks on the United States and its allies. The name BianLian refers to the concept of face changing associated with Chinese theatre, but apart from the name, nothing else indicates the group's possible homeland.

**RECENT ACTIVITY:** Ongoing attacks on businesses and government bodies operating in English-speaking areas. Recently, targets especially in the United States, but also European and Australian organisations have fallen victim to the group.

**METHODS AND TACTICS:** The group targets vulnerable targets using VPNs or cloud services and uses ransomware of its own creation based on the Go programming language. Especially the customers of the US company Sonicwall have been targeted, due to weaknesses found in the provider's VPN application.

## EVASIVE GELSENIUM

**DESCRIPTION:** Evasive Gelsenium is a cyberespionage group, an APT group that has been operating since 2014, whose operations are directed at authorities, education and electronics manufacturers in East Asia and the Middle East. The group has enormous technical capacity and programming expertise, which is why the group has managed to carry out long-term operations without being exposed.

**RECENT ACTIVITY:** Focused its long-running espionage operation on Southeast Asian governments in 2022-2023. The targets are especially the Tibetan region, the administration of Taiwan and the Uyghurs.

**METHODS AND TACTICS:** Uses backdoors in their operations and is a very advanced APT group.







## RUSSIA CONTINUES ITS HYBRID OPERATIONS ONLINE

Russia and actors affiliated with Russia have continued not only their military operations in Ukraine, but also their hybrid influencing operations around the world. There is no universally accepted definition of hybrid influencing, but in a broad sense it usually refers to forms of hostile influencing that may aim to destabilise the political system or society as a whole. The means of hybrid influencing can be, for example, political, diplomatic, economic and military, as well as information and cyber influencing. In particular, Russia's online hybrid influencing through information and cyber means has been strong during the summer. Russia's influence has mainly taken place in two ways: cyberattacks and spreading fake news. Other hybrid influencing is also taking place, and only the tip of the iceberg is likely to be visible.

In the summer, the Russians have been active cyber attackers. For example, the hacktivist group NoName057(16) has been conducting almost daily DDoS attacks. The targets have been states defined by the group as Russophobic that support the war effort in Ukraine. The selected victims include, for example, Finland, Lithuania and Italy, where attacks have targeted not only public but also private sector actors. Another major player that has been active over the summer is Anonymous Sudan – also a particularly specialised with denial-of-service attacks. The group has attacked the European Investment Bank and threatened Israel, among others, with cyberattacks. The group tries to present itself as Sudanese and Islamist, but experts say it is a Russian actor. According to its own words, it has also carried out more advanced operations. In early July, Anonymous Sudan announced that it had obtained the credentials of more than 30 million Microsoft users and was willing to sell it for a fee of \$50,000. Microsoft has denied what happened, and it is likely that there has been no data breach. The third significant actor is Turla, often linked to the Russian FSB, which in the summer has sought to attack the Ukrainian Armed Forces with spyware.

Another form of Russian influence online is the spread of fake news, which has continued both in Europe and around the world. In June, an information operation was uncovered in France to spread pro-Russian content. Themes included downplaying sanctions against Russia, accusing Ukraine of Nazism, and Western countries about Russophobia. The allegations were spread through fake news sites which imitated major newspapers, such as Le Monde and Le Figaro, as well as websites that resembled the websites of the French authorities in appearance. Content was also shared through fake accounts. Another noteworthy case is the burning of the Koran in Sweden, which has caused great opposition in the Islamic world.

Swedish authorities have discovered a Russian information operation behind it, which has fed fake news to the world and sought to incite hatred towards Sweden. Fake news has been made in Arabic and it has been spread through the sanctioned news sites Russia Today and Sputnik.

Different actors seem to have different ways of working and achieving different goals. For example, NoName seems to be mainly aimed at making public propaganda profits from states that support Ukraine, and it openly acts on behalf of Russia. Anonymous Sudan, on the other hand, acts more covertly and denies any links to Russia, but carries out attacks in Russian interests. Turla is conducting more technically demanding operations, and its recent operations seem to be mainly related to the war in Ukraine. What is significant about Russian cyber activities is the blurring of the boundaries between private and state-controlled activities. The aforementioned groups carry out ideological attacks, but in addition to the sheer maximum destructive effect, they also make ransom demands. Surprising objects have also been seen. Anonymous Sudan has targeted Kenya, among others, which on the face of it seems like a random target. However, an explanatory factor may be the Kenyan president's comments about Russia, accusing Russia of stabbing Africa in the back by withdrawing from the grain deal. The incident shows how long Russia's arm is, and how even surprising targets the Russians are willing to spend their resources on. Russia also has enough cyber capacity for non-priority targets, as it is likely that the focus of cyber operations will remain in Ukraine.

Taken as a whole, Russia's hybrid online operations through cyberattacks and disinformation campaigns leave a mixed picture. For example, the impact of denial-of-service attacks is often quite small and temporary. On the other hand, the country also has advanced units capable of demanding operations. Russia's fake news, on the other hand, may have been thought of as a thing of the past, because with the war in Ukraine, Russia's potential to get its own narrative through in the West is practically non-existent. Instead, Russia has turned its attention elsewhere, to third countries, which Russia may still be able to persuade to its side. It is essential to recognise the cyber and online environment as just one of the many fields in which Russia seeks to exert influence. The threat posed by this action should not be underestimated or forgotten.





## CHILDREN'S SMART DEVICES AFFECT LEARNING AND INCREASE CYBER THREATS

For almost every citizen, smart devices are a part of the daily activities. The biggest deviations from this are the youngest and oldest citizens. However, we are moving in a direction where different smart devices are being used at an increasingly younger age. Today, even small children are very skilled users of smart devices. At the latest, when school starts, the child often gets their first mobile phone or other smart device, such as a smart watch, with which they can communicate with their parents during school days. Children also quickly learn to search for content on smart devices through applications, and the watchful eye of parents does not always see if the child inadvertently wanders over to content that is not suitable for children.

Spanish doctor of neuropsychology, Alvaro Bilbao, has published a study on the connections between children's increased screen time and children's neuropsychological symptoms. According to Bilbao, children's risk of depression, addictions and concentration disorders increases with the time they spend in front of mobile screens in their early childhood. Based on the research, screen time on mobile devices especially for children under the age of six should be significantly limited or even banned completely. Other bodies, such as the American Pediatric Society, has made this same six-year recommendation.

The United Nations Educational, Scientific and Cultural Organisation UNESCO has also demanded stricter restrictions on smart devices in schools. Like Bilbao, the report of the UNESCO highlights how the use of smartphones causes concentration disorders and negatively affect to the learning and well-being of children and young people. The mere presence of phones has been found to have a negative effect on learning. The UNESCO report calls for better regulation of educational technology. Inadequate monitoring of educational technology also exposes children to many security threats,

such as cyberattacks and cyberbullying. According to the UNESCO report, information technology should only be used in lessons for a purpose that is really useful for learning. When phones are included in classes, it easily leads to their use in matters not related to studying, which in turn has a negative effect on remembering and understanding.

Almost a quarter of countries have currently banned the use of phones in their schools completely. In Finland, too, the government has clarified guidelines and regulations on the use of smart phones in schools. In Finland, teachers are currently allowed to prohibit the use of phones and collect them if their use is perceived as disturbing. However, it is challenging to enforce a complete ban on the use of phones, for example during recess. Today, many teachers may also be annoyed by unauthorised filming and other kinds of harassment.

However, the existence of a mobile phone or some other smart device gives peace of mind to both the child and the guardian. However, when purchasing a smart device, it is good to make sure that the phone or device is still supported by its manufacturer, so that the phone receives the necessary security fixes and updates. It is also the parents' task to supervise how minors use their phones and what kind of applications they can download to the smart devices. For example, many cybercriminals use game applications specifically aimed at children to enable their crimes. However, it is relatively easy to put various application and usage restrictions on children's phones these days. The task of adults is also to act as the child's most important media educator, to teach the correct use of smart devices and online etiquette, because children do not always know what a risky activity is. Cybersecurity training should be a key element when starting to use smart devices. The challenge is that not many parents have recognised the risks of digital devices.



## SIM SWAPPING AS A TOOL FOR CYBER CRIMINALS

SIM card hijacking so-called SIM-swapping attacks have become more common internationally at the same pace as the number of smartphones has grown. With that growth, more are lost in everyday use and their use, for example, in two-step authentication has increased. Attacks on mobile devices often go unnoticed until it is likely too late. A successful SIM swap enables the attacker to access, among other things, the victim's message history, contact information, emails, social media profiles, bank IDs and all the services that are linked to the hijacked phone number. Most of the time, the main goal of SIM swapping is financial. The attack is based on exploiting the weaknesses of two-step authentication based on SMS messages.

The SIM card activates calls, text messages and data services in the phone, and each SIM card has unique identifiers that connect it to only one mobile phone. Moving the SIM card to another phone also automatically transfers the card's mobile services to the new device. It is not always necessary to transfer the physical card, but mobile services can be easily transferred from one SIM card to another. The operation is commonplace for telecom operators, and this is done, for example, if the phone is lost or stolen. This is precisely why mobile devices are susceptible to SIM swaps. In these attacks, the fraudster gains control of the phone number using the victim's identity and other personal information, causing the phone operator to associate the victim's number with the SIM card in the fraudster's possession. Once successful, the scammer is able to bypass all SMS-based two-step authentication for user accounts using that number. When a SIM card is hijacked, all the user's information, starting with the phone number, is transferred to a new card, and the original one stops working.

Ransomware group Lapsus\$ has been reported to have used the SIM swapping method in a variety of ways in its data breaches and ransomware attacks. Lapsus\$ is a

loosely affiliated cybercriminal group consisting of young English and Brazilians whose main motivation for their activities seems to be gaining fame. At the end of July, US security authorities published an extensive report on the group's operating methods and attack methods. In its previous crimes, the group has used SIM swaps as an attack method, especially to gain access to the target company's internal network to steal confidential information, such as source code, user IDs or customer data. Some of the SIM swaps carried out by the group have been done directly through customer management tools hijacked from telecom operators. In some of its attacks, the group used insiders of telecom operators or target organisations by paying them for services and information. The fact that a group of cybercriminals like this has been able to break into companies' valuable information so easily by using identification based on text messages has caused concern.

The hijacking of SIM cards does not only affect the individual mobile device user but can also be the most common entry technique for a cybercriminal group to a selected target. A certain amount of information about the target is required to carry out the attacks. This information can be accessed relatively easily just by buying the information from the black markets or collecting the information from social media profiles. SIM swapping relies heavily on collecting as much personal data as possible. Indeed, many who use this method of cyberattack benefit from all the unique information of the potential victim, which social media platforms and information-combining combo lists circulating in the black markets are full of. Scammers also often sift through social media profiles for clues, such as pet names, that can be used as password recovery security questions and used to hijack phones. For example, a simple method works to prevent the hijacking of SIM cards: switching from two-step authentication based on text messages to passwordless alternatives or separate authentication applications.





## CYBERATTACKS ARE BECOMING FASTER AND THE DEMAND FOR UPDATES IS GETTING MORE URGENT

Last week, security firm Sophos released a report examining the recent trends in cyberattacks. According to the report both attack detection and the speed at which threat actors act have significantly developed over the past year. In practice, this is reflected in the shortened "dwell-time" that the attacker spends on the target organisation's systems before carrying out the actual attack or being caught. According to the report, the current shortened time to a median of about eight days may indicate that advanced interception and detection capabilities have reduced attackers' ability to prepare attacks. On the other hand, an equally likely explanation is that it is the attackers' actions that have evolved and become more efficient, enabling a faster cycle of operations. The latter idea is also supported by other statistics on the ever-increasing number of successful attacks - on the other hand, it is difficult to obtain statistics on failed attacks. In any case, the reduced dwell time offers the defending organisation less opportunity to detect the actor that has penetrated the network and reduce the impact of the attack. Even if it is a result of developed defensive capabilities, this will inevitably lead to criminals sooner or later reacting by speeding up their operations, so that the end result will in any case be cyberattacks that will be carried out more quickly.

In addition to accelerated operations, there has recently been some attention on how quickly cyber attackers exploit vulnerabilities in target systems, both found by themselves and those that are publicly communicated. Typically, it doesn't take many days after a vulnerability is discovered before fast-reacting threat actors are ready to use an attack method or tool that exploits it. Both the shortened dwell time and the accelerating pace at which

vulnerabilities are exploited challenge organisations to take a more active and action-oriented approach to cybersecurity. System scans once a week or installing new updates every few weeks are no longer enough, as the attack can be planned, prepared and executed within this period. In addition, many organisations have much older and overlooked vulnerabilities that are already common knowledge.

Accelerating the pace of updates is also a need noticed by many application providers. For example, Google announced in August that it would increase the frequency of updates to the Chrome browser to once a week instead of every other week. Similarly, Apple has introduced more frequent instant updates this year that specifically address security vulnerabilities. Many application providers are also actively releasing updates when new vulnerabilities are discovered. However, how quickly these updates reach organisations is another matter. It can take up to several days after an update is released to respond to it, providing attackers with a valuable window of time for the vulnerability to exploit.

Active vulnerability monitoring and the installation of updates are therefore increasingly central to the implementation of cybersecurity. In addition to misusing user IDs, exploiting known vulnerabilities is one of the most common ways to carry out cyberattacks, and at worst, un-patched security vulnerabilities provide the threat actor with easy and free access to the organisation's systems. As the pace at which threat actors can carry out their operations is also accelerating, the need to remain aware of vulnerabilities in their own systems and the updates available to them is constantly emphasised. At best, a timely update can prevent an ongoing intrusion, and at a minimum, it limits how easily an attacker can gain access to systems. ■





A PASSION  
FOR A SAFE  
CYBER WORLD



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

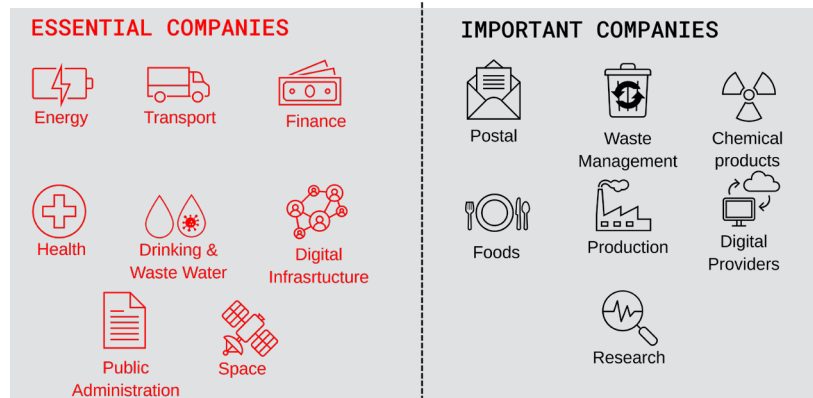
## Analysis

### 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.

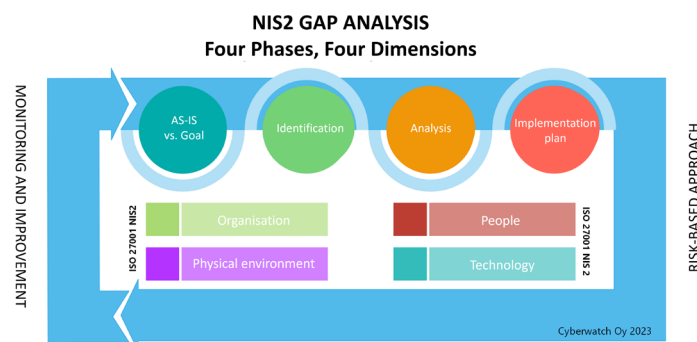
NIS2 cyber security directive concerns the following fields:



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

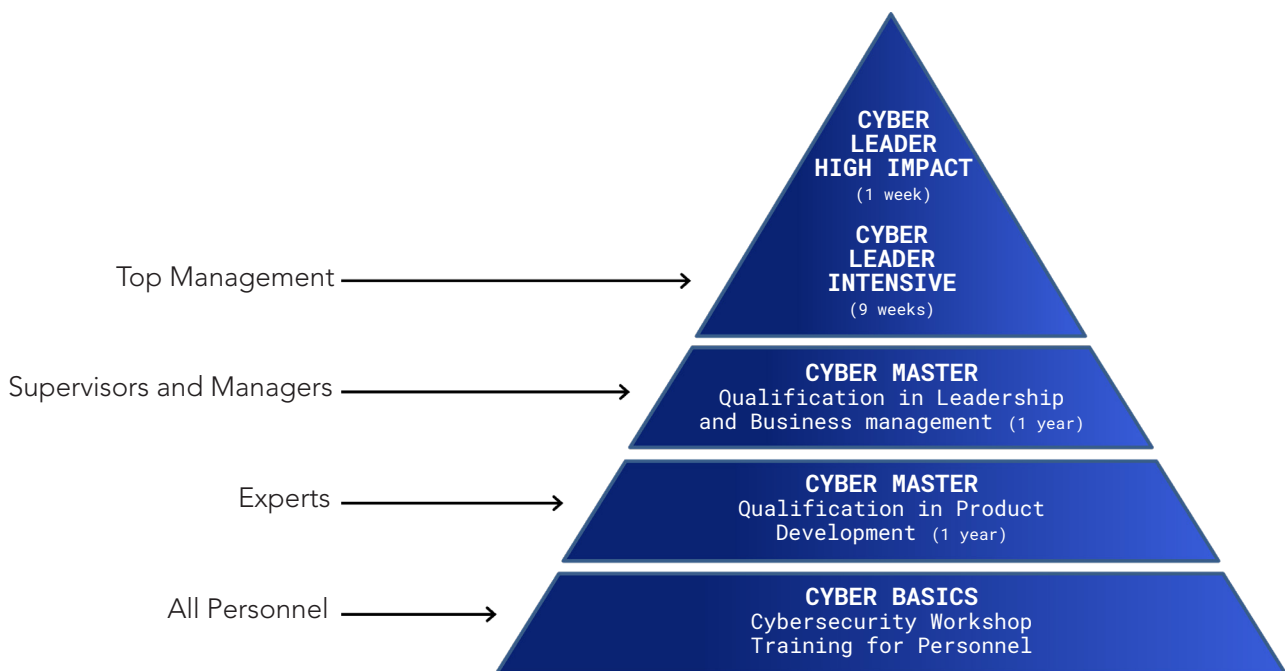
### Training and Competency Development

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](mailto:aapo@cyberwatchfinland.fi)  
[ake@cyberwatchfinland.fi](mailto:ake@cyberwatchfinland.fi)  
[myynti@cyberwatchfinland.fi](mailto:myynti@cyberwatchfinland.fi)