Cyberwatch Finland

MAGAZINE 3/2025

Global Politics is Challenging Our Future Cyber Defence

Cybersecurity is Built by Small Actions and Management of Large Concepts

Our Aim is to Add Cyber Capabilities in the World

CONTENT

Cyberwatch Finland
MAGAZINE 3/2025

Cyberwatch MAGAZINE

PUBLISHER Cyberwatch Oy
Nuijamiestentie 5 C
Helsinki, Finland

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

LAYOUT PuulaMedia / Mari Riepponen
ILLUSTRATIONS AdobeStock
PRINT Scanseri Oy, Helsinki

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

The Cyber World Is Changing Constantly

The global security seems increasingly unstable: the war in Ukraine shows no end, European air traffic is being actively disrupted, the development of the global economy is full of uncertainty, domestic extremist movements are gaining strength in many countries, and the crisis in the Middle East continues. The list could go on and on. The European Union and NATO have made significant decisions to strengthen their defence. This will hopefully have positive effects on our economy and European unity, as well as on the ability to secure the digital structures of our society. Cybersecurity is part of all processes and systems related to our security.

If you ask Finns what threatens us the most, the answer will come quickly. The majority mention Russia and some mention China as well. Our security thinking is still based on traditional threat assumptions, which are not wrong. The complex global interdependent world is difficult to grasp. Hybrid threats are recognized at some level, but it is difficult to form a comprehensive and reliable situational picture from the mixture of phenomena of different degrees. For example, artificial intelligence can be used to produce fake news faster and more credible than ever before.

Many academics say that the worst threat is not Russia or China, but weak economic development in Europe. The idea is shattering. Political decisions to strengthen our military defence and comprehensive security will not succeed without the economic conditions. Poor economic development may indeed be our greatest threat. The most critical core of a modern digital society is stable economic development and its impact on people's sense of security and our opportunities to develop our defence system. The means to correct and improve our national economic situation are not simple. The US president's divisive tariff policy is hampering the opportunities of an export-driven country. Therefore, the EU's joint efforts are increasingly important. In addition, trade relations with countries in Asia and the Global South must be maintained. Economic security will continue to be one of the cornerstones of our comprehensive security approach.

When asked what is changing, all experts mention the importance of artificial intelligence, quantum computing, drone warfare and space. Few can crystallize the change into concrete new phenomena or mega trends. The most significant change from the cybersecurity point of view may be the combination of military and civilian technologies into so-called dual-use products. Another strategic-level change is people's need to stay in touch with their loved ones. Our resilience requires functional communication systems, even in crisis situations.

The lessons learned from Ukraine can be combined with the opportunities that came with the new technology and thereby find solutions to the future challenges of critical communications. In the future, perhaps the most important requirement for critical infrastructure will be digital and physical resilience. Systems must be well protected, remembering that there is no such thing as a completely reliable system. In national critical infrastructure, data is also at the heart of all operations. The transfer of data between different actors is a central part of communications and the operation of digital systems. We must be able to build a networked, cyber-secure society that uses alternative forms of data transfer and advanced technologies.

The strong economic foundation of our country requires innovation and the ability to better utilize the opportunities offered by technology, without forgetting the key role of people. The winners will be those who view security challenges holistically and are agile in adapting to the continuous change in our security environment. Developing defence and security brings new employment opportunities and opens new markets in a networked world, while at the same time strengthening our economy. So, let's make cybersecurity more of an opportunity than a threat in the future, it will also keep our economy on a solid foundation.

RISTO RAJALA &
PETER SUND

A Strong and Coherent EU Is the Best Safeguard in Times of Global Instability

The gradual weakening of the multilateral treaty system, intensifying regional conflicts, and the instability and unpredictability of major powers currently shape international relations. This instability also affects digitalized societies in many ways. Cybercrime is on the rise, and in addition to traditional financially motivated criminal groups, state actors are increasingly involved. Growing attention must be paid to the security and reliability of technologies and the intentions of their developers. At the same time, the availability of software, hardware components, microchips, and minerals essential for digitalized critical infrastructure and broader economic activity is increasingly governed by politics rather than business, with states controlling supply chains not hesitating to leverage their strengths.

The trend of liberalizing international trade, which gained momentum after the Cold War, began to reverse in the 2010s as negotiations within the World Trade Organization failed to yield results and states began erecting trade barriers. It also became clear that not all states involved in trade liberalization acted in good faith to increase mutual dependencies aimed at securing peace. Instead, some sought to create one-sided dependencies, for example in fossil energy and critical minerals, which could be used as instruments of power politics. The intensifying

competition and strained relations between major powers, and especially Russia's full-scale invasion of Ukraine in 2022, marked a definitive shift from liberalized trade relations to an era of "geoeconomics," where economics and geopolitics are deeply intertwined.

Strengthening Europe's Digital Sovereignty

The European Union and its member states have struggled to adapt to the growing importance of geopolitics in shaping international relations. Historically, this is understandable, as European integration has been built on liberalizing trade between member states, creating mutual dependencies, and establishing common rules and institutions. The EU is undeniably a major power in trade policy, with its large single market and strong competences traditionally yielding convincing results. However, the actions of Donald Trump's second administration, which began in January 2025, and its various ripple effects have repeatedly prevented the Union from leveraging its strengths and painfully exposed its weaknesses.

Europe's current security architecture is entirely dependent on the United States' military presence, security guarantees, and defense materials. The U.S. also plays a critical role in supporting Ukraine's defense and enabling security solutions for the country. The Trump administration has demonstrated an unprecedented willingness to pressure Europe, particularly by linking economic and even regulatory issues to security. The practically one-sided "trade agreement" between the EU and the U.S. allowed the U.S. to raise tariffs on nearly all categories of goods, and EU member states saw no alternative but to accept the unfavorable deal. In addition to transatlantic challenges, the EU is unable to safeguard its interests in relations with China and Russia, both of which seek to undermine the Union's credibility and unity.

Europe's digital infrastructure is also heavily dependent on microchips, hardware components, and software produced in the United States. Europeans spend a significant portion of their time on U.S.-based social media platforms. In hindsight, it can be argued that Europeans did not fully grasp the significance of digital technology development when markets were still emerging. Dependencies on U.S.-produced software and technology have become increasingly evident this year, not only in terms of service availability and reliability but also regarding confidentiality. U.S. technologies are essential not only for business continuity but also for innovation and competitiveness—AI computing, for example, relies on graphics processors.

The EU's challenges are compounded by over a decade of economic stagnation and lagging in the development and financing of transformative technologies on a global scale. However, the EU and its member states now appear to be waking up to reality. Defense investments are increasing and are expected to accelerate due to the flexibility introduced in the EU's fiscal rules (Stability and Growth Pact) regarding defense spending, and the SAFE instrument offering favorable loans to member states for defense development.

The Commission's proposal for the Multiannual Financial Framework (MFF) for 2028–2034, published in summer 2025, would significantly shift EU spending toward defense, security, and technology. If implemented, it would be a crucial step in addressing the Union's major challenges. The proposal is promising for cybersecurity, suggesting the establishment of a €400 billion Competitiveness Fund to boost strategic investments in security, innovation, digital technologies, low-carbon solutions, and the bioeconomy—of which €125 billion would be allocated to defense and security, and €55 billion to digital leadership. Other key cybersecurity-related funding programs, such as Horizon Europe, would also be expanded. Maintaining the proposed funding levels for technology and security is essential for Europe's technological sovereignty, competitiveness, and defense capabilities. In particular, Competitiveness Fund resources should be directed toward supporting the development of modern and critical technological solutions in Europe and their demand in the single market.

The CSAM Proposal Threatens to Derail the Efforts to Pursue Technological Sovereignty

Despite promising plans, a legislative proposal currently under consideration in EU institutions threatens to undermine efforts toward European digital sovereignty, jeopardizing cybersecurity and Europeans' right to confidential communication and privacy. The proposal, prepared over several years by the Commission, aims to combat child sexual abuse material (CSAM) online. Several member states have made compromise proposals during their Council presidencies, none of which have gained the required qualified majority.

While the proposal has a legitimate and urgent goal—protecting children who are victims—it employs methods that are both ineffective and highly problematic. Unlike Poland's previous compromise, Denmark's latest proposal reverts to the deeply problematic path of Hungary's earlier version. Denmark reintroduces mandatory identification requirements and forced consent mechanisms for users of communication and storage services, which cannot be considered permissible under EU law. This would lead to broad, indiscriminate surveillance of communication content by authorities.

End-to-end encryption ensures that only the sender and intended recipients can read or analyze messages. Service providers or other entities cannot access message content, even if messages pass through their systems. Whether surveillance occurs before or after encryption is irrelevant - it still constitutes circumvention of encryption and the right to private communication. Notably, Denmark's proposal excludes security and defense authorities, acknowledging the risks of such mechanisms in communication services. Providers must be able to choose their encryption technologies and agree on their use with customers, as the core purpose of end-to-end encryption is to ensure the confidentiality and integrity of customer-owned data. This is also vital for Finland's overall security, economic resilience, and supply security. Trade secrets, such as customer and product development data, are daily targets of espionage and sabotage, threatening both economic security and supply resilience.

Online sexual violence can be divided into two categories: dissemination of abuse material and grooming. Grooming involves manipulative behavior where an adult builds trust with a minor to prepare them for sexual exploitation. The most critical target for protecting children is the production of abuse material, where the minor is directly victimized. Denmark's proposal excludes grooming prevention. It's important to note that perpetrators use the same communication services as legitimate users. Switching services is easy, making vague risk assessments of providers ineffective.

In spring 2024, Europol and the heads of member states' law enforcement agencies issued a joint declaration aiming to break encryption and eliminate privacy in communication. Initially framed around CSAM prevention, the proposal was expanded in the EU's internal security strategy (ProtectEU) published on April 8, 2025, to include security authorities' access to all electronic information. This clearly targets end-to-end encryption and other encrypted digital data, such as trade secrets, which are foundational to business value and economic viability. Policymakers are often misled into believing such measures are necessary for crime prevention. While the appeal of "enhancing security" is strong, in the digital world it often becomes a double-edged sword. Weakening encryption, restricting its use, or forcing companies to cooperate for "lawful access" has repeatedly led to reduced security, harming innocent users rather than criminals.

It's worth noting the recent developments in the United Kingdom, where under the Investigatory Powers Act, authorities demanded the breaking of end-to-end encryption. As a result, Apple removed strong encryption from services for all UK-based users. This clearly weakens overall security. U.S. agencies such as CISA, FBI, and now the FTC have explicitly warned American tech providers against weakening user security for these very reasons. The threats posed by encryption-breaking proposals to Europe's digital

security are not theoretical; they are clearly visible in global examples.

NATO's Defence Spending Target Should Be Harnessed to Strengthen Cybersecurity

Russia's ongoing aggression and the United States' increasingly strict demands for higher defence spending have placed NATO in an unprecedented situation. At the NATO summit in The Hague in summer 2025, member states agreed that in the future, they should allocate 5% of their gross domestic product (GDP) to defence. Of this, 3.5% would be dedicated to military defence expenditures, and 1.5% to other defence-supporting investments in infrastructure and industry.

It is essential that a significant portion of future investments—particularly within the 1.5% allocated to defence-supporting measures—be directed toward strengthening cybersecurity in civil society, especially within businesses. For example, in Finland, key sectors critical to societal functioning each face cybersecurity investment gaps of up to €150 million compared to the maturity levels required by current conditions and legislation. Cybersecurity is a core component of modern security, alongside police, rescue services, and national defence. However, the means to strengthen cybersecurity largely lie outside the hands of security authorities and instead rest with other administrative sectors and, above all, the business community. The vast majority of digital data, information and communication systems, and production systems are managed by private companies.

It is also noteworthy that the success of military defence depends heavily on the reliability of civilian digital infrastructure, such as electricity and communication networks, data centres, and production control systems.

When promoting the protection of digital society, attention must be turned to businesses and their ability to manage digital risks. There is a strong case for significantly expanding policy measures to support companies in maintaining cybersecurity. Successful examples of impactful policy actions include the 2023 cybersecurity voucher used to strengthen the security of companies critical to national preparedness, and EU grant-based support for the adoption of modern cybersecurity risk management tools in businesses. Supporting the deployment of the most advanced cybersecurity solutions in companies would enhance the reliability of critical infrastructure, business continuity, and the preservation of corporate assets—thus reinforcing the foundations of economic growth.

Meeting NATO's defence spending requirements will demand painful political decisions from Finland, especially given the already strained state of public finances. It is therefore crucial that any increases in spending are made in a balanced way, maximizing societal benefits. Investments in civil society's cybersecurity are a prerequisite for defending a modern, digital society. So far, the direction in Finland has unfortunately been the opposite. Although Prime Minister Orpo's government has pledged not to cut security spending, the administrative sector responsible for cybersecurity—the Ministry of Transport and Communications—has faced budget cuts, unlike other key security-related sectors. It is imperative that improving civil society's cybersecurity as part of NATO's defence spending goals becomes a prominent issue in the 2027 parliamentary elections.

The cybersecurity industry plays a key role in protecting societies, individuals, and businesses from the effects of instability in the global digital environment. Finnish Information Security Cluster actively advocates for increased funding to improve cybersecurity, emphasizing the importance of measures aimed at protecting civil society and strengthening the operating conditions of companies that provide cybersecurity products, services, and solutions.

AUTHORS:

PETER SUND

CEO
Finnish Information Security Cluster (FISC)

Technology Industries of Finland

Jukka Rapo

RISTO RAJALA

Advisor
Finnish Information Security Cluster (FISC)

Technology Industries of Finland

The Future Challenges And Solutions of Critical Communication in Modern Societies

Introduction

Technology is developing at a faster pace than ever before, while the war in Ukraine and others elsewhere are morbidly highlighting the challenges that critical infrastructure faces in such difficult conditions. New regulation is trying to meet these challenges, especially in the EU, but often also imposes new ones in the process. A key part of critical infrastructure is critical communication, the future of which is very complex, but that does not mean it cannot be prepared for. There are lessons to be learned from the conflicts around the world and emerging technologies should be put to use based on them.

When imagining the requirements for future products, it is best to start by looking at what they are right now. The logical first step is to check the legislation, in this case the NIS2 directive and Finland's recently passed cyber law that stems from it. The most relevant requirements for communication technologies include protection of communication networks and systems, separation of said systems from any outside environments, access control and regular updates. Last but not least, the systems have to be usable in times of serious disturbances and unusual conditions as well. This calls for resilience, both digital and physical.

Key Lessons from the War in Ukraine

The war in Ukraine has first and foremost shown us how diverse the methods employed in modern warfare are, and how quickly they can develop. At the start of the war Russia was attacking anything and everything, but since then the attacks in cyberspace have become more precise and targeted. Much more emphasis is placed on gathering intelligence and tailoring the attacks for each target to achieve the best possible results. They are also more tightly connected to military and information operations than before.

Ukraine had already improved their cyber capabilites during the years leading up to the full-scale invasion of 2022. For example, automated process control systems and their corresponding cybersecurity mechanisms were deployed. These systems have successfully provided a high level of protection and functionality under conditions of armed aggression. In addition, the largest operators agreed on permitting national roaming to ensure the resilience of networks. According to Ukrainian sources, another key aspect of a successful cyber defense is, perhaps a little ironically, the effective use of offensive cyber capabilites. It seems that attack is the best defense in cyberspace as well. The key ideas behind this thought are deterrence, pre-emptive strikes and effective retaliation.

The most vulnerable targets for Russian cyber-attacks have been different parts of Ukrainian critical infrastructure. Attacks have been going on for over a decade now, and new ones are constantly being conducted. The most effective operations have resulted in widespread blackouts, complete shutdown of communications networks and growing public distrust on both governmental institutions and private companies alike. This highlights the immense importance of resilience in civilian infrastructure. Although not all attacks in the cyber domain are directed at civilians, they often provide easier targets due to more relaxed security measures. The adoption of standardized (unique) hardware and infrastructure within organizations significantly enhances resilience and facilitates rapid recovery following cyber incidents. The importance of co-operation and support from the private sector, volunteers and especially partner states has been proven throughout the war in Ukraine. Because of the war, Russia

and Ukraine are developing roughly 10 times faster than non-warring states when it comes to cyberwarfare, so keeping track of developments within their conflict is the key to staying up-to-date on current cyber capabilities and trends.

The cyber dimension seems to fulfil a supporting role in kinetic conflicts worldwide, while also acting as a method of hybrid warfare. Recently it has above all else acted as a key component of information operations. When it comes to Russia, it seems that most cyber resources are directed against countries supporting Ukraine, rather than Ukraine itself. Just like within Ukraine, communication systems seem to be a priority target for Russian operations in nations supporting Ukraine as well. Even if a ceasefire in Ukraine would come into effect, Russia would continue its cyber operations, which it tries to maintain below the threshold of traditional warfare. As such, national resilience needs to be strengthened even further.

Russia's information operations outside Ukraine have likewise been targeting civilian societies in an attempt to change public opinion towards narratives that Russia could better exploit. Russia makes extensive use of artificial intelligence in its information operations to produce endless content for social media and other similar platforms. The platforms spread lies by instructing AI models to mass-produce false narratives – for example, to create thousands of articles containing disinformation and to publish them online. Russia is also using AI for reconnaissance and exploitation in cyber operations. Despite the use of AI and other developments in technology, human factor remains the most vulnerable link in the cybersecurity and managing vulnerabilities chain. Raising cyber awareness and maintaining a high level of cyber hygiene among personnel remains essential. Phishing attacks, malware deployment, and the creation of botnets are among Russia's leading tactics for information theft and disruption of information and communication systems at this stage of the conflict.

Future Communication Solutions as a Strategic Capability in a Global Context

In a conflict situation, whether it be kinetic or cyber in nature, eventually an attack will succeed in disabling at least some parts of a system. When that happens, resilience steps in. First and foremost, systems need to have backups in case of a failure. Secondly, repairing them has to happen quickly.

Resilience is not limited to just physical infrastructure either. The importance of digital resilience is still often overlooked, but in a modern digitised society it is a crucial part of security. The aim of digital resilience is to have the ability to maintain operations in exceptional conditions with minimal effort. In an ideal situation, this capability is already included into the system during the design phase. If the system already exists, it is important to identify the most critical parts for continuity of service and how the system reacts to disturbances. If the system is critical, and it does not stay operational during a disruption, it needs to be improved. The support of reliable vendors and a well-funtioning supply chain are critical.

Dual-use systems improve resilience, because interchangeable components and personnel between civilian and military system maintenance can greatly improve the speed at which systems are repaired. If something can be used both by the military and the civilian society, that means there will be more of them around, making sure the logistics chains are not stretched too thin. It can also provide an opportunity to transfer a system from civilian to military use or the other way around and means parts from one can be used in the other, greatly improving the scalability of military systems during crises. Regardless of whether the system is in civilian or military use, it is important to remember that effective resilience requires personnel in addition to components to be close by, otherwise repairs cannot be completed quickly.

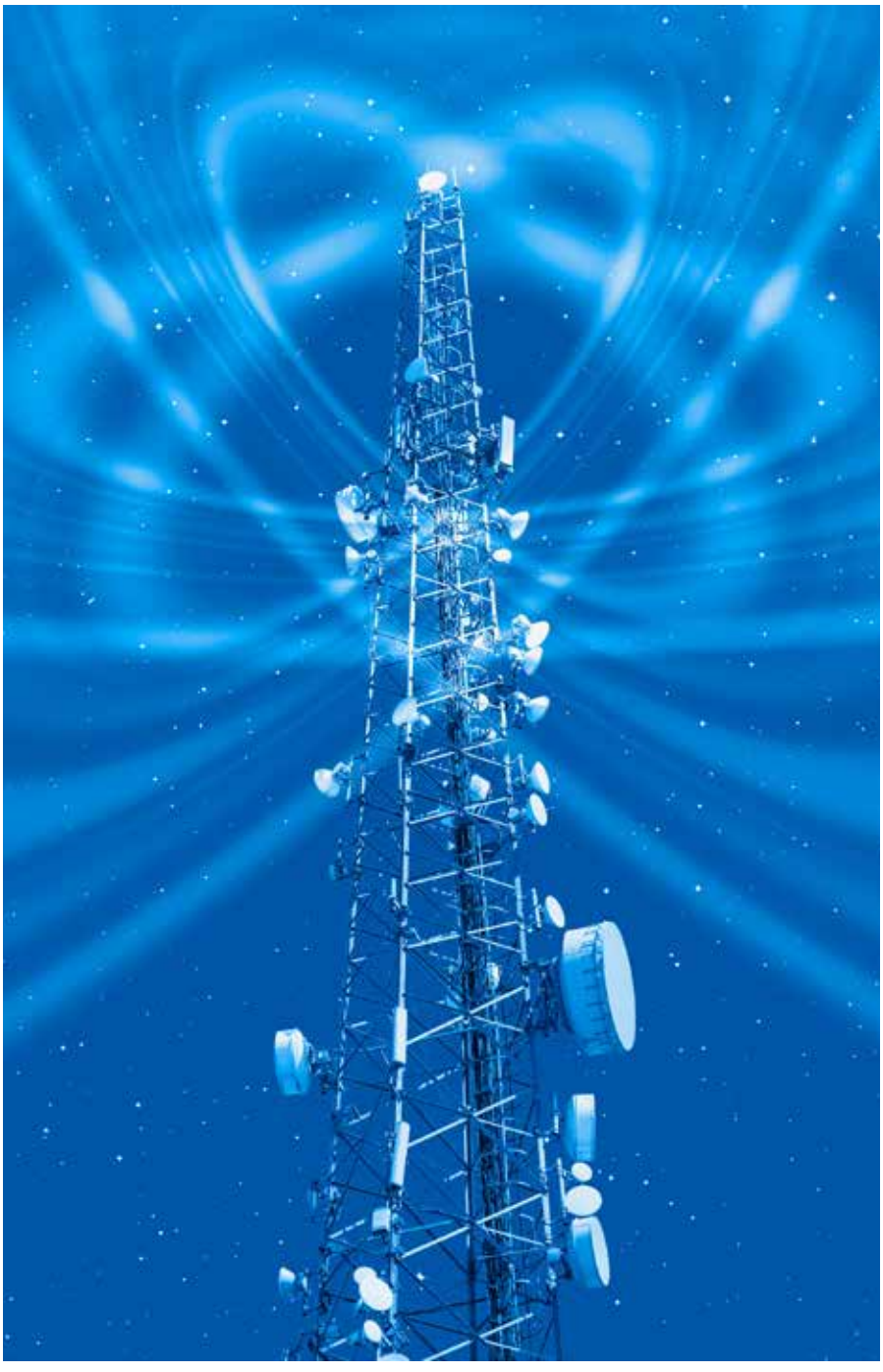
Dual-use products are not without issues, namely the differing requirements of security when comparing traditional civilian and military use cases, but developing such products does still provide a competitive edge to any companies that wish to succeed in the current geopolitical environment. What needs to be kept in mind, however, is the risk-based approach to such products. That is what the cyber law and the Critical Entities Resilience Directive call for, but it is also the key to understanding the security requirements of military use cases. All data should not be processed on the same device, since gaining access to it would then instantly provide an attacker with everything. This is true for critical infrastructure as well, and separating systems from one another can be an effective way to prevent single threats from taking out entire capabilities. At the same time, especially when looking at the war in Ukraine, it has become clear that civilian networks are widely used as backup systems in military operations. Another cost-efficient solution for a backup system for the new Virve 2.0 could be a network utilising a low-band spectrum.

Systems need to be customisable for different use cases and targets. Since different users will obviously have different use cases for the product, it must be easy to adapt it to those needs. When developing a dual-use product from the ground up, this has to be kept in mind. Quite often it can mean that a system used primarily by the civilian society needs to have its security improved when it is transferred into military

use. Network slicing can be a part of the solution for critical services – delivering priority service, lower latency and faster speeds. The slicing could possibly be used to increase security as well, by cutting off the part of the network used by the military from its civilian counterpart, for example.

The Open Radio Access Network is an emerging technology that can be used to optimise the radio network with the help of open interfaces and an advanced division model for radio network functions. For example, some of the base station's functions can be transferred to the cloud so that it can distribute the available radio capacity more efficiently to other base stations. The concept would be useful in the dynamically changing combat situations of military operations. By integrating AI into the RAN architecture, the use of radio resources and frequency management can be optimised and the overall efficiency of the system improved by enhancing adaptation to dynamically changing telecommunications and frequency conditions. The real-time operations of the AI-RAN system place additional demands on the implementation and performance of AI algorithms due to resource and latency limitations, which can be somewhat mitigated by edge computing. It means performing some of the computation "at the edge", in other words near the physical origin of the information, instead of in the cloud. It can help reduce the strain on networks and speed up processes, since less data is sent to a data center and back.

A key requirement when it comes to communication is reliability. When looking at the war in Ukraine, disruption of communications has been a recurring theme during the conflict. Methods that would be more resistant to jamming and other forms of disruption could be real gamechangers on the battlefields of Ukraine and any future conflict areas. AI-integration can help tackle these issues, since AI-driven networks can enhance network efficiency, reduce latency, and enable seamless connectivity across satellite, aerial, and terrestrial networks. Perhaps the most significant factor influencing the development of AI is quantum computing. That is because unlike normal computers, quantum computers can investigate all the possible solutions at the same time thanks to superposition and quantum entanglement. Quantum computers also have a way to dramatically cut down the time it takes to solve the mathematical problems currently used to cypher communication from thousands of years to hours or even minutes. Suffice to say, the ability of quantum computers to fairly easily break nearly every type of encryption method currently in use has huge implications for cybersecurity. The best possible way to prepare for this is probably going to be to look for "crypto-agile" systems—ones where switching from one form of encryption to another is easy. This way it will be much easier to keep up with the undoubtedly rapid updates to quantum-resistant encryption methods.



Another requirement for future communications systems will be the ability to divide information into different categories of protection, for example into public, confidential and secret. Those could easily represent civilian, critical infrastructure and military actors and their requirements for communication security. It might not be necessary for civilian communication to be protected against quantum threats as early on as military or critical infrastructure, since these two are more likely to be targeted by hostile actors with early quantum capabilities. The requirements for security are different in other aspects as well, so it is something to keep in mind when designing dual-use systems.

Cloud technologies could improve resilience and allow for more dual-use items to be easily integrated into defense solutions, with tactical edge computing further improving resilience and making sure connections are not overloaded. Thus cloud services could be one part in a solution for developing more flexible systems and structures. The scalability of cloud networks could enable unprecedented situational awareness, support for autonomous systems, realtime target tracking and more powerful simulation tools. That said, not everything can be solved by cloud services. Even with a completely separate cloud system, security will be a big concern, and secret data might be best kept out of the cloud completely. Therefore the need for more traditional communication solutions remains.

Another key communications technology is the use of satellites, which has seen explosive growth in the past couple of years. At the forefront of this change is the emergence of non-terrestrial networks (NTNs)—networks that completely circumvent conventional ground infrastructure. These days, satellite organizations supply high-speed access to even the most remote and underserved regions of the world by providing connectivity from space. This has already been proven critical to Ukraine's military command structure, and it does not take a lot of

imagination to picture how important NTNs are in areas where critical infrastructure on the ground has been partially or completely destroyed.

Suffice to say, NTNs are going to become an almost mandatory backup system for both civilian and military communication during future crises. Satellite-based solutions could also be the best possible backup system for the communication of Finnish authorities, since a traditional radio network is much easier to destroy—especially if the network infrastructure is located close to other critical infrastructure. The Finnish Defence Forces is already investing into space technology during the coming years, so communication systems could be a part of this development.

Strengthening National Resilience

When combining the lessons learned from Ukraine and elsewhere with the possibilities of emerging technology, it is possible to deduce solutions for the future challenges of critical communication in modern societies. Perhaps the most important requirement of any future critical infrastructure is resilience, both digital and physical. Especially based on the experiences from the war in Ukraine, that resilience should include resistance to electronic warfare operations.

Systems need to be well protected of course, but a fool-proof system does not exist. When something eventually does go wrong, there need to be backup systems available, and the repair or replacement of the original has to happen quickly. The way to facilitate this is through ensuring components and personnel are close enough to enable a quick response. Dual-use systems are one way to achieve this, since the expertise of personnel and interchangeable components can then be borrowed from civilian systems to military ones and the other way around.

Dual-use systems do provide challenges too. Ensuring sufficient security for military use of civilian products is the most prominent one. Testing the systems and practicing with them can also prove to be more challenging than what it would be with strictly military systems, but fortunately Finland has a long history of close co-operation between the military and other parts of the society. Co-operation between the private and public sectors must be seamless, and concepts that have been proven to work, such as national roaming in Ukraine, should be prepared in advance to enable quick reactions. Unnecessary political obstacles for resilience should also be removed when establishing trusted partnerships with companies. Only through the common multi-actor-model of companies and the public sector can digital sovereignty be ensured at all times.

Future systems need to be highly customisable as well, because the operational environment is in a constant state of change. This is observed best in Ukraine, where the development cycle of drones is getting quicker and quicker. Prominent trends in technology, such as AI, 5G/6G, satellites, cloud services or quantum computing, are going to provide unique opportunities and challenges for communications systems. It is therefore imperative to pay attention to the development of these key capabilities in the near future. Being able to adapt systems already in use for new innovations and use cases is a massive benefit both financially and in terms of time when compared to the prospect of acquiring completely new hardware and software every time a new capability is developed. Critical infrastructure operators must build a networked, cyber-secure entity that uses alternative forms of data transfer and advanced technologies to achieve the necessary resilience at different levels of operations.

REFERENCES/SOURCES

https://www.comsoc.org/publications/ctn/predicting-future-communications-technologies

https://www.hs.fi/alueet/art-2000011306235.html

https://www.avenga.com/magazine/satellite-technology-bringing-satellite-in-the-palm-of-the-hand/

https://satcube.com/news/current-satcom-trends-shaping-the-future-of-connectivity?gad_source=1&gad_campaignid=21079435382&gclid=EAIaIQobChMIpNOMseiijgMVvluRBR1C2iy1EAAYASAAEgICY_D_BwE

https://www.techtarget.com/searchdatacenter/definition/edge-computing

https://www.telekom.com/en/company/management-unplugged/details/satellite-communication-a-powerful-addition-to-europe-s-digital-future-1093760

https://spacenews.com/shaking-up-satcom-the-time-is-now-for-radical-innovation-in-satellite-communications/

https://www.critical-entities-resilience-directive.com/

https://www.telia.fi/yrityksille/artikkelit/artikkeli/tutustu-digitaaliseen-huolto varmuuteen

https://gofore.com/kuka-suojelee-meita-kriisissa-jossa-kysytaan-digitaalista-huoltovarmuutta/

https://www.dna.fi/yrityksille/blogi/-/blogs/5g-ssa-voit-viipaloida-yritys verkkosi-mita-se-kaytannossa-tarkoittaa

https://thebulletin.org/2025/03/russian-networks-flood-the-internet-with-propaganda-aiming-to-corrupt-ai-chatbots/

https://viestiupseeriyhdistys.fi/wp-content/uploads/2021/08/VM-2-2021.pdf

https://viestiupseeriyhdistys.fi/lehti/viestimies-4-2023/

https://issuu.com/viestimies/docs/vm_2024-1

https://issuu.com/viestimies/docs/viestimies_1_2025/30

https://issuu.com/viestimies/docs/viestimies_2_2025

https://ai-ran.org/

https://www.erillisverkot.fi/virve2-0/?gad_source=1&gad_campaignid=16178890739&gclid=EAIaIQobChMI8ontv6PQjwMVNQiiAx3n2Bf-EAAYASAAEgJvh_D_BwE

Cyberwatch analysis of the war in Ukraine

Cyberwatch Weekly Reviews

Presentations of the Cyber Breakfast 2025

MATTHIAS WASINGER

The Illusion of Transparency: Data vs. Intelligence on the Battlefield

Abstract:

Hybrid warfare integrates both military and non-military tactics, leveraging AI, cyberspace, and the information realm as force multipliers. Cyberspace and the information realm serve as a domain and battlefield, while AI accelerates decision-making and disinformation. Modern surveillance fosters a perception of a ”transparent battlefield,” yet raw data is not actionable intelligence and understanding adversarial intent remains the challenge. The West faces a dilemma: adversaries exploit AI without restraint, while ethical and legal limits hinder its own capabilities. Regardless, AI's use in hybrid warfare is inevitable, and will require strategic adaptation to maintain a competitive edge.

Bottom-line-up-front:

AI, cyberspace, and the information realm shape the 21st-century battlefield, creating the illusion of total transparency. However, while data is abundant, true intelligence—the understanding of intent—remains elusive, forcing the West to choose between ethical AI restraint and strategic disadvantage.

Problem statement:

How to understand the claim for transparency on the battlefield in a digitised world?

So what?:

Western military and political leadership must prioritise the integration of AI, not merely for data gathering, but for producing and exploiting actionable Intel in real-time—including understanding adversarial intent. This requires collaboration with private tech companies under strict ethical and legal frameworks to ensure strategic advantage without sacrificing accountability. Simultaneously, analogue systems must be maintained to safeguard against technological failure or compromise.

Modern Conflicts, Data and Intel

21st-century conflict is increasingly shaped by the dynamics of hybrid warfare, an approach that integrates conventional military operations with non-military means.[1] Hybrid warfare employs all instruments of national power, including economic, diplomatic, informational, and military capabilities, alongside semi-governmental and private entities that act as complementary effectors. In this complex environment, artificial intelligence (AI), cyberspace, and the information domain emerge as critical enablers and force multipliers, fostering the perception of a so-called "transparent battlefield." Most recently, the employment of Unmanned Aerial Vehicles (UAVs) on both sides in Russia's war against Ukraine have evoked claims of a vitreous battlefield.[2] Likewise, similar conclusions were drawn following the 2020 Nagorno-Karabakh war between Armenia and Azerbaijan. What was overlooked in this case was the fact that Türkiye provided Azerbaijan with a "Turkish All-Inclusive" package, covering training, education, materiel, intelligence (Intel), and battle damage assessment capabilities.[3]

However, the reality is that transparency remains largely illusory, and claims of such are nothing new. More than 100 years ago, Giulio Douhet forecasted in his well-renowned opus "Command of the Air" that there would be no more hiding on the battlefield, no more distinction between civilian and military targets, and no more covert movement of forces, due to air power's overwhelming impact.[4] Similarly, cyber warfare and spectrum warfare–the control, development, and use of advanced electromagnetic (EM) spectrum technologies for strategic advantage and mission success in military engagements and intelligence gathering–tempted humankind to assume battlefield omniscience.[5]

The assumption is that modern reconnaissance capabilities have rendered covert movement impossible. Yet, this perspective overlooks a fundamental distinction between raw data and actionable Intel. In none of these examples did a belligerent achieve decision-making superiority due to enhanced data collection–which is, ultimately, the outcome of either quantitative and/or qualitative or innovative sensors. Raw data does not automatically bequeath automatic comprehension of an opposing force's intent. Such comprehension comes from superiority in Intel production, dissemination, and exploitation, leading to superiority in decision-making that made a difference on the battlefield. Raw data is the foundation of Intel, not the basis for decisive action.[6]

While AI, cyberspace, and information technologies excel in collecting and processing vast amounts of data, they often fall short in interpreting the intentions of the actors. The ability to gather data is not synonymous with understanding the strategic objectives, motivations, or psychological drivers behind adversarial actions. As a result, the so-called transparent battlefield is, in reality, an incomplete and sometimes misleading construct.[7]

The Ukrainian Armed Forces' so-called Kursk incursion in 2024 illustrates this. The Russian Armed Forces had reams of raw data; however, the operation's purpose caught the Russians off guard. Ukrainian forces were not invisible to Russian sensors, yet due to a lack of understanding about their purpose and intent, the Ukrainian Armed Forces penetrated Russian territory and seized, to Vladimir Putin's embarrassment, a swathe of territory in the Kursk region. Consequently, this Ukrainian operation not only raised attention in the information domain; it fixed Russian forces for months and even led to the deployment of approximately 12,000 North Korean soldiers in the region.

Reinforcing the fallacy of the transparent battlefield, it is unclear—despite Russian claims—whether the Russian Armed Forces have managed to fully clear the incursion at the time of writing.[8]

Intel as Foundation for Decision-Making

Understanding an opponent's intent within means and capabilities is vital for planning on all levels of command, within and without the military realm. Indeed, the peculiarity of human decision-makers makes it almost impossible to fully understand or even predict an actor's intent with certainty. Humankind is often unpredictable. Consequently, all Intel is, to a certain extent, a best guess, based on historic data, best (or worst) practices, patterns and probabilities. It is an assumption that has to be validated perpetually.[9] However, this best guess provides planners in all realms and on all levels of command with a foundation for developing appropriate measures. Intel is, therefore, a vital means to situational understanding.

In this context, cyberspace plays a dual role in modern conflict: it is both an artificially created domain and an active battlefield. When combined with the information realm, cyberspace becomes a crucial factor in all phases of hybrid warfare. AI, in particular, accelerates the spread of information and disinformation, enabling rapid decision-making and influencing adversarial strategies.

Since human processing capabilities are limited by nature, both AI and cyberspace have the potential to alter the quality and velocity of Intel development. So far, and in the Western world, both are mainly employed to gather information and data.[10] They set the scene for Intel development or the visualisation of collected data rather than creating an exploitable understanding of opposing

forces' intent. Without this critical understanding, AI and cyberspace might *evolutionise* rather than warfare; in other words, they may provide more of the same but at volume and velocity instead of changing the rules of the game.

In this regard, cyberspace and AI might be game-changers. Suppose raw data can be processed more accurately to develop and disseminate an operational understanding of opposing forces' intent in real-time; Intel can be developed not only based on historic data but in correlation with an actor's most recent deeds and most likely understanding of their necessities and urgencies; the employment of AI that considers ethical, moral and legal standards accordingly so AI can be embedded in mission command principles. Then, the scene is set for superiority in decision-making; indeed, potentially for all warring parties.

"I Need Some Intel, and I Need It Fast"

Technological advances, such as uncrewed systems, satellites, and cyberspace, mean that decision-makers and modern deployed armed forces are well-supplied with data. The challenge nowadays is how to filter the Big Data for the irrelevant from the relevant information in a timely manner. Collected data must be processed to gain valuable information, which has to be evaluated and turned into intelligence and knowledge. This theoretically simple process presents profound challenges. Processing data requires analytical and technical support to ensure currency, and the human information computing capability is the limiting factor in this process.[11] Consequently, AI may mitigate this human limitation or even render it obsolete.

For example, regarding AI, the People's Republic of China (PRC), is superior to the U.S. in setting the benchmark for quantum supremacy by combining AI and Quantum Computing as a quantum intelligence service.[12] Processing, evaluating information, and disseminating intelligence on time are preconditions for decision-making superiority; they allow the creation of multiple dilemmas for an opponent. However, technology itself is an opportunity for, as well as a potential threat to, the respective *superior power.* It is heavily linked to a capable industrial base and technology but bears the risk of creating dependence on technology and its weak points.[13]

Threat

Relying on high technology runs a risk of creating a kind of defence-in-

dustrial dependence on other global powers. Indeed, to a certain extent, this applies to all major powers—never mind small states. The PRC, for example, is attempting to address this issue through its "Made in China 2025" state plan.[14] Whereas substantial progress toward self-reliance has been made regarding ship-building, aerospace, and missile technology, the PRC still falls short, for example, in producing semiconductors. Since the latter are vital, especially regarding computing, AI and cyberoperations, this is a serious shortfall in preparation for or ensuring deterrence against war; it becomes an existential threat in (sustainable) war.

Even though the U.S. has built the most developed defence-industrial base, it lacks, interestingly, the same shortfalls, namely dependence on semiconductor imports.[15] Measures like the CHIPS and Science Acts were taken. However, it will take years to achieve full self-reliance.[16] In consequence, the U.S., as the leading Western military power, runs the same potential risk as its global main adversary, the PRC. This is particularly surprising since the so-called Western way of warfare (in fact, the U.S. way) is based on possessing the technological edge, especially in the long run.

Losing its strategic technological advantage will, inevitably, urge the U.S. to fundamentally adapt its doctrinal approach to warfare. This is in stark contrast to the PRC, which might—nothing more than—fall back on its default doctrines and strategic approaches to warfare, which were based on quantitatively overwhelming an opponent, combined with a willingness to bear substantial human and materiel losses.[17]

Besides, and this is valid for all powers, high technology is a vulnerability by itself. AI systems can be hacked, influenced and even turned against their human masters. Indeed, there might be technical solutions to these issues. Nevertheless, there will remain a certain risk despite defence industry claims of game-changing AI security.[18]

Consequently, and as with many developments in military technology throughout history, AI bears risks for all belligerents. Contrary to previous developments, AI is not solely a military asset that dwells in the military domain. Private corporates are critical players in modern conflict, often connected to battlefields via cyberspace. In times when global companies' annual financial surplus exceeds the (defence) budgets of major European countries, one must not neglect these "independent non-state" actors.[19] There are several reasons why US President Trump surrounds himself with so-called "TechBros".[20] Elon Musk, Mark Zuckerberg, and Jeff Bezos, undoubtedly, supported his campaign financially. Even more, their respective companies collect vast amounts of global data and hold profoundly influential opinions.

Like mercenaries in past times, these actors might go (or change) to the highest bidder, pose an inherent risk to data and AI security, and, ultimately, further monetise warfare. Those owning cyberspace as a means of data transportation and storing, possessing data, and having access to AI-assisted decision-making systems, eventually influence (or dictate) the course and outcome of wars. Tech giants could conceivably transform into warlords, and war become a means to an economic end.

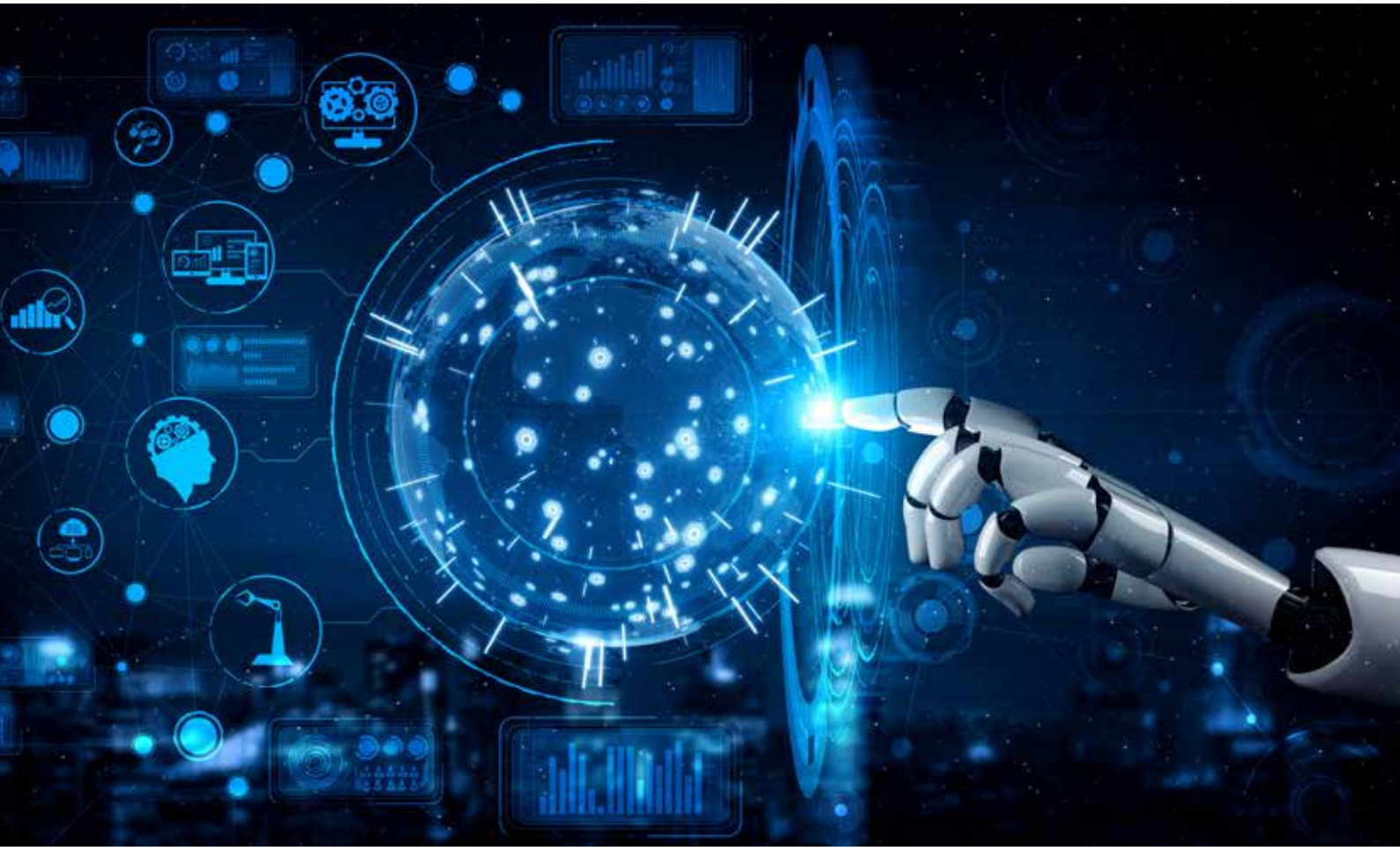
Opportunity

On the flip side, embracing emerging and disruptive technologies bears several undeniable advantages. Algorithms and machines can work almost incessantly and thus replace the limiting (human) factor in running the Intel cycle and decision-making process. Military approaches and doctrines can be automatically assessed, patterns in human decision-making understood via automated Operations Research (OR),[21] likelihood and probability recognised, and plausible decisions forecasted. AI can increase the speed of these processes, and also optimise processes that are, as things stand right now, restricted by limited human processing capacities.

A full and unrestricted employment of AI could upend the strategic paradigm, similar to the strategic upheaval following the advent of nuclear weapons: a technological leap forward that, according to the U.S., saved hundreds of thousands of lives while still killing tens of thousands.[22] Like the nuclear bomb, AI could contribute to a strategic parity of the sort that once led to relative peace and stability. Additionally, if handled appropriately, AI has the potential to add sanity to the (irrational) human endeavour of war.[23]

Indeed, there will still be no certainty! Human behaviour is unpredictable. It is influenced by very human characteristics such as pride, fear, fury and anxiety. Humanity is full of irrationality. Whereas European leaders assessed Russia's aggression as presumably irrational due to the "change through rapprochement", Russia and President Vladimir Putin see themselves in an inevitable struggle against Western imperialism and for national autonomy.[24] However, the so-called global West's assumptions were rather emotional than rational.

AI follows the rational. Russia, and especially Vladimir Putin, knows and follows the drill. Russia's policymakers sit down every time the West stands up.[25] AI acknowledges their, seemingly, endless record of broken treaties and agreements. AI understands Russia's misbehaviour, including but not limited to, the Helsinki Accords, the UN Charter, the Intermediate-Range Nuclear Forces



Treaty, the Budapest Memorandum, and the Minsk Treaties. Contrary to human beings, AI understands, acknowledges and considers this proven record of broken accords.[26] AI concludes without emotions and hope; it uses Operational Research, best practice, with high speed. It does so on the strategic level, where the employable means are by far broader than on the operational or tactical level. The lower the level of command, the more limited the field of options becomes. However, this influences human assessments even more than AI-facilitated decision-making. Consequently, AI has the potential to enable superiority in decision-making on all levels of command.

So, if commanders and decision-makers require Intel quickly, AI-supported processes will be key. Their speed, adaptability, and capacity to process vast amounts of data in real time, if harnessed systematically may provide modern forces with a significant operational edge. However, the fundamental nature of warfare—with its uncertainty, unpredictability, and potential for disruption—demands built-in redundancies.[27] Just as human forces can be misled or overwhelmed, technological systems can also be neutralised, compromised, or exploited by adversaries. Therefore, analogue fallback options will always be necessary to ensure resilience in the face of digital failure. While timely and accurate Intel is vital, once the fog of war descends, even delayed or partial intelligence is preferable to none at all. Consequently, even if AI supports decision-making, there will be an inherent need for trained and educated staff officers capable of operating if technology fails.

The Art of the Deal…

Policies for AI employment are often concern-driven rather than technologically (r-)evolution-oriented— especially in the global West. One of the main concerns revolves around the ethical contemplation that AI lacks morality, and, therefore, might act against the so-called Western standards. Most European nations find themselves in the European Union (EU), which defines itself as a Union of values. Human dignity, liberty, democracy, equality, the rule of law and adherence to human rights are enshrined in Article 2 of the Treaty of the European Union.[28] Whereas this treaty solely binds EU member states, one may assume that most Western nations ascribe to these values, at least verbally. Nevertheless, European nations have to adhere to these values, especially in warfare. This is particularly true if

one accepts that military employment is ultimately meant to project a nation's or community's values and morale.[29]

The argument circulates around the ethical considerations that AI lacks moral judgment. AI has no soul, no consciousness, and no sense of (morally) right or wrong. An algorithm follows pre-set rules within a defined framework. However, AI is more complex than commonly assumed. Decisions are not taken binarily. AI works with assessed probabilities. Moreover, it operates within a framework and rules that humans set. In short, the expected and acceptable outcome depends on the quality, conciseness, and clarity of the framework and the rules. Moreover, there's the question of accountability for machine failure and violations of the laws of war.

Nevertheless, as superficially reasonable as it seems, the argument seems out of context. It assumes human beings take conscious, reasonable, ethically and morally correct decisions. As a matter of fact, we humans have an obnoxious record in adhering to rules, agreements and values developed by and for ourselves. Humankind defines ethics and moral; and humankind abandons, disregards and, eventually, redefines ethics and morals as it deems appropriate or, moreover, useful. Merely within the last 100 years, and without the support of AI, humankind initiated and, at times, morally justified, colonialisation, slavery, human trafficking, child abuse, genocide, ethnic cleansing, two world wars, more than 100 wars,[30] and the invention plus the (twice) employment of nuclear weapons. As empiricism illustrates, and with this (even tightly framed!) historical human record, it appears hypocritical to neglect AI due to ethical and moral apprehensions.

Additionally, there's the question of accountability. Human-made law applies to human beings. However, legal accountability in war matters because it protects lives, delivers justice, upholds international norms, and helps prevent future violence.[31] Yet, algorithms can't be made accountable for violations of (international) law. From the author's point of view, what appears to be a show-stopper for AI employment in warfare is another fig leaf for not employing contemporary technology. Indeed, there is accountability. Certainly, AI might decide on life or death on a human's behalf. However, so does, the end of the day, a smart

bomb. No doubt, the shooter/operator/employer is to be held accountable for the caused effect. Voices in the Western world that blame the defence industry or weapon-delivering states for harm done in war are both irrational and a minority vote. Yet, there is a connection from arms production to deaths on the ground, and unlike industrialists commanders and soldiers in the field are often legitimately held accountable for their deeds. One can contextualise this divergence in accountability through the humble landmine, mines don't care about ethics and morals. Moreover, not all countries have even signed the related Ottawa Convention. Some even left the Convention. Nevertheless, both mines and mine producers are hardly legally held accountable for more than 4,500 annual casualties worldwide. The forces positioning the mines are those held liable!

Moreover, even if AI makes decisions, it does so within a framework set by humans. Whether the human is in or out of the loop, there is still, at a certain point, human oversight and "rule setting." AI employment does not automatically mean we will see a Terminator-style "Skynet" scenario.[32] Consequently, it remains questionable whether the probability of losing control over an algorithm is higher than suffering from ungovernable subordinates.

Furthermore, belligerent powers' comparably lower adherence to Western-style standards must evoke remarkable concern. The aforementioned values and concerns do not pre-emptively impact their thoughts or actions regarding AI. Nevertheless, both the PRC and Russia introduced ethical rules for AI employment. Yet, they do so from a different perspective and with an unalike purpose. Antagonists set these rules to align AI with political purposes, not to endanger political leadership. Ethics and morals are used to ensure a regime's survivability.[33, 34] So, the wording might be the same; however, it follows a different rationale.

Use It or Lose It

The integration of AI into warfare presents both strategic opportunities and existential risk. While adversaries like the PRC and Russia adopt AI with few (or simply different) ethical reservations, the Western community of nations faces constraints rooted in legal and moral principles, potentially leading to operational disadvantages. Despite advances in reconnaissance and AI, the notion of a fully "transparent battlefield" remains largely illusory—data alone does not equate to actionable intelligence. Human intent, shaped by unpredictable behaviour, still eludes even the most advanced systems. Yet from today's vantage point, the battlefield increasingly *appears* transparent. This perception, however, is expected to be challenged as technology evolves.

Intel—not raw data—remains the foundation for decision-making, underscoring the continuing importance of human interpretation. AI can accelerate data processing, but it must be framed within human-made ethical and accountability boundaries. Furthermore, reliance on high-tech systems introduces vulnerabilities; they can fail, be compromised, or exploited. Therefore, analogue fallback options remain vital to maintain operational resilience. As AI reshapes command and control, its success will depend on how well humans define its rules and integrate it into established military doctrines. Ultimately, AI may offer an edge—but only when balanced with enduring principles of human oversight, ethical governance, and redundancy in system design.

AUTHOR:

Matthias Wasinger is a Colonel (GS) in the Austrian Armed Forces. He holds a Magister in Military Leadership (Theresan Military Academy), a master's degree in Operational Studies (US Army Command and General Staff College), and a PhD in Interdisciplinary Studies (University of Vienna). He has served both internationally and nationally at all levels of command. He is also the founder and editor-in-chief of The Defence Horizon Journal. The views expressed in this paper are the author's alone and do not reflect or relate to any of the abovementioned organisations.

MATTHIAS WASINGER

REFERENCES/SOURCES

1 Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats, "Hybrid Warfare - Hybrid CoE - the European Centre of Excellence for Countering Hybrid Threats," last modified April 08, 2025, https://www.hybridcoe.fi/hybrid-warfare/.

2 The Economist, "The Added Dangers of Fighting in Ukraine When Everything Is Visible," The Economist, February 06, 2025, accessed May 23, 2025, https://www.economist.com/europe/2025/02/06/the-added-dangers-of-fighting-in-ukraine-when-everything-is-visible.

3 Botakoz Kazbek, "The Turkish "All-Inclusive" Package of Military Service and the Nagorny Karabakh Case 2020," TDHJ.org, January 10, 2022, accessed May 23, 2025, https://tdhj.org/blog/post/turkish-all-inclusive-military-service/.

4 Giulio Douhet, The Command of the Air, USAF warrior studies (Washington, D.C.: Air Force History and Museums Program, 1942), 10.

5 AUSA, "The Transparent Battlefield: Combat Training Centres Sharpen Unit Tactics for High-Tech Fight," last modified June 25, 2024, https://www.ausa.org/articles/transparent-battlefield-combat-training-centers-sharpen-unit-tactics-high-tech-fight.

6 Thierry Balzacq and Ronald R. Krebs, The Oxford Handbook of Grand Strategy, 1st. ed. (Oxford: Oxford University Press, 2021).

7 US Naval War College, "LibGuides: Intelligence Studies: Types of Intelligence Collection," last modified May 23, 2025, https://usnwc.libguides.com/c.php?g=494120&p=3381426&utm.

8 Gareth Jones, "Russia Says Last Ukrainian Troops Expelled from Kursk Region, Kyiv Denies Assertion," April 26, 2025, accessed April 27, 2025, https://www.reuters.com/world/europe/putin-hails-end-ukraines-kursk-incursion-with-expulsion-last-ukrainian-troops-2025-04-26/.

9 Stig K. Andersen, "Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference," Artificial Intelligence 48, no. 1 (1991), https://doi.org/10.1016/0004-3702(91)90084-W.

10 Christian Nitzl et al., "The Use of Artificial Intelligence in Military Intelligence: An Experimental Investigation of Added Value in the Analysis Process" (2024).

11 Antonella C. Vilasi, "The Intelligence Cycle," Open Journal of Political Science 08, no. 01 (2018), https://doi.org/10.4236/ojps.2018.81003.

12 Jonathan Ward, China's Vision of Victory (The Atlas Publishing and Media Company, 2019), 86.

13 Richard A. Poisel, Information Warfare and Electronic Warfare Systems (Artech House, 2013), 26-50.

14 Vladimir Zamorin, "Contribution of the Chinese Military-Industrial Complex to the "Made in China 2025" State Plan," Far Eastern Affairs 51, no. 002 (2023), https://doi.org/10.21557/FEA.86159334.

15 Sujai Shivakumar and Charles Wessner, Semiconductors and National Defence: What Are the Stakes? (2022), https://www.csis.org/analysis/semiconductors-and-national-defense-what-are-stakes.

16 Kashif Anwar, "The Battle for Global Chip Dominance: The U.S. "CHIPS and Science Act"," TDHJ.org, August 22, 2022, accessed May 24, 2025, https://tdhj.org/blog/post/usa-chips-science-act/.

17 US Army War College - Publications, "Adapting US Defence Strategy to Great-Power Competition," last modified May 24, 2025, https://publications.armywarcollege.edu/News/Display/Article/4129357/adapting-us-defense-strategy-to-great-power-competition/.

18 Pillar Security, "Pillar Security Raises $9M to Help Enterprises Build and Run Secure AI Software," Yahoo Finance, April 16, 2025, accessed May 23, 2025, https://finance.yahoo.com/news/pillar-security-raises-9m-help-131500361.html?guccounter=2.

19 Johns Hopkins SAIS, "How Private Tech Companies Are Reshaping Great Power Competition," last modified February 21, 2024, https://sais.jhu.edu/kissinger/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition.

20 Jeffrey Goldfarb, "Breakingviews - Silicon Valley Daredevils Ride or Die with Trump," Reuters Media, July 18, 2024, accessed May 24, 2025, https://www.reuters.com/breakingviews/silicon-valley-daredevils-ride-or-die-with-trump-2024-07-17/.

21 "OR is defined as the application of scientific and mathematical methods to provide decision-makers with a quantitative basis for decisions regarding operations under their control. This approach focuses on enhancing the efficiency and performance of manpower, machinery, equipment, and policies within military operations." A. Lakshani Pramodhya, "The History of Operations Research," OR Society, June 21, 2022, https://ors.soc.pdn.ac.lk/blog/history-of-operation-research.

22 Joseph H. Paulin, "America's Decision to Drop the Atomic Bomb on Japan," accessed May 24, 2025, https://repository.lsu.edu/cgi/viewcontent.cgi?article=4078&context=gradschool_theses&utm.

23 Alex Cope, "When AI Meets the Laws of War | IE Insights," IE Insights, October 03, 2024, accessed May 24, 2025, https://www.ie.edu/insights/articles/when-ai-meets-the-laws-of-war/.

24 Der Pragmaticus, "Putins Hass Auf Den Westen | Der Pragmaticus," Der Pragmaticus Verlag AG, February 17, 2023, accessed May 24, 2025, https://www.derpragmaticus.com/r/russland-westen?.

25 Dermot Nolan, "Through Audacity and Arms: How Europe Can Restrain Russia," TDHJ.org, March 04, 2024, accessed May 24, 2025, https://tdhj.org/blog/post/audacity-arms-europe-russia/.

26 Smith K. Khare et al., "Emotion Recognition and Artificial Intelligence: A Systematic Review (2014–2023) And Research Recommendations," Information Fusion 102 (2024), https://doi.org/10.1016/j.inffus.2023.102019, https://www.sciencedirect.com/science/article/pii/S1566253523003354.

27 Alexander Schäbler, "1+1 ≠ 2: Digital Friction, Uncertainty, and the Limits of Technological Determinism," TDHJ.org, May 22, 2025, accessed May 23, 2025, https://tdhj.org/blog/post/digital-friction-technology-determinism/.

28 European Union Treaties, "Consolidated Version of the Treaty on European Union," European Union Treaties, last modified May 15, 2025, https://www.legislation.gov.uk/eut/teu/article/2.

29 Matthias Wasinger, "A Revolution in Military Ideas: The Continuing Importance of the Enlightenment in an Age of Technological Autonomy," The Strategy Bridge, December 09, 2019, accessed May 24, 2025, https://thestrategybridge.org/the-bridge/2019/12/9/a-revolution-in-military-ideas-the-continuing-impotance-of-the-enlightenment-in-an-age-of-technological-autonomy.

30 Again, depending on the set rules, the numbers range from 100 to 1,000.

31 International Committee of the Red Cross, "Investigating and Prosecuting Serious Violations: An Important Tool Against Impunity," last modified October 14, 2024, https://www.icrc.org/en/statement/79-UN-crimes-against-humanity-investigating-and-prosecuting-serious-violations-tool-against-impunity.

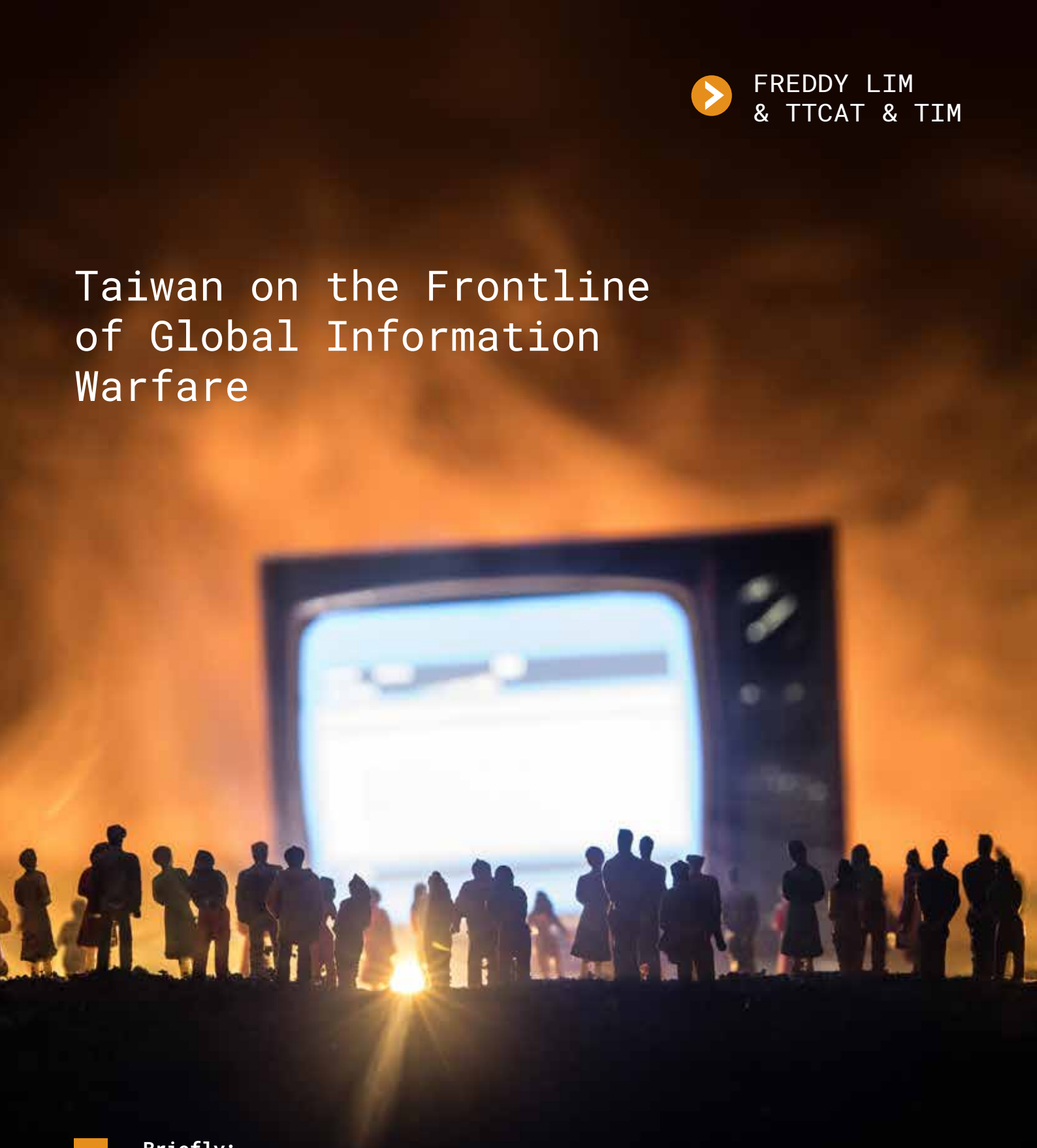
32 James Black et al., "Strategic Competition in the Age of AI: Emerging Risks and Opportunities from Military Use of Artificial Intelligence," RAND, 2024, 6-8., accessed May 23, 2025, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3200/RRA3295-1/RAND_RRA3295-1.pdf.

33 Masha Borak, "Inside Safe City, Moscow's AI Surveillance Dystopia," WIRED, February 6, 2023, accessed May 23, 2025, https://www.wired.com/story/moscow-safe-city-ntechlab/.

34 Samuel Yang and Chris Fung Bill Zhou, "AI Ethics: Overview (China)," last modified January 20, 2025, https://www.chinalawvision.com/2025/01/digital-economy-ai/ai-ethics-overview-china/?.

FREDDY LIM
& TTCAT & TIM

Taiwan on the Frontline of Global Information Warfare



Briefly:

In today's interconnected world, the online ecosystem has become a double-edged sword, fostering both unprecedented connectivity and alarming levels of polarization. Across the globe, from Finland to far-flung nations, societies are grappling with the consequences of information silos, algorithmic biases, and the deliberate spread of divisive narratives. These polarization phenomena can be the natural outgrowth of online algorithms that push users towards extreme content[1], or they can stem from other deeply rooted social factors, or even from sophisticated information warfare campaigns waged by foreign regimes. This global issue poses a significant challenge to democratic discourse and societal cohesion, creating fertile ground for external actors to exploit existing divisions.

Reports from the University of Gothenburg have consistently identified Taiwan as the country most severely impacted by foreign disinformation for several consecutive years.[2] Trends show that China is also waging similar information attacks against more democracies and sharing its mechanisms and experiences with other authoritarian regimes.

Given this, we believe it is crucial to share our lessons from Taiwan in confronting China's information warfare. By reviewing what we have learned with our democratic allies, we can hopefully better counter these challenges together.

Exploiting Discord to Advance Geopolitical Goals

China has demonstrably capitalized on this global polarization, particularly in its strategic pursuit of annexing Taiwan. Beijing's approach involves a multi-pronged information warfare strategy designed to influence public opinion, erode democratic institutions, and ultimately achieve "unification" without direct military conflict.

At its core, China's information warfare in Taiwan aims to achieve several high-level strategic objectives:

- **Promote "unification" (annexation):** Beijing consistently pushes narratives that portray the economic and technological opportunities offered by closer ties with China as highly attractive for Taiwanese citizens. Messages like "Both sides of the Strait are one family" culturally, are frequently used to foster a sense of shared identity.
- **Undermine attachment to Taiwan's independent, democratic status quo:** A significant part of the strategy involves discrediting Taiwan's democratic government and electoral processes. Narratives frequently suggest that democracy itself is chaotic and fails to serve ordinary people, the government is corrupt, and the electoral system is fraudulent.
- **Create anxiety about the strategic situation:** China seeks to instill a sense of futility regarding resistance. This is achieved through messages emphasizing the overwhelming strength of the Chinese military compared to Taiwan's smaller, less capable forces, and by sowing doubt about the willingness of the United States to come to Taiwan's aid.

These objectives can be summarized as: "Unification is attractive, democracy isn't working for you, and anyway resistance is futile." If a sufficient number of Taiwanese citizens come to believe these core messages, Beijing hopes they will vote for pro-China politicians, paving the way for annexation without a fight.

Beyond these primary goals, China also aims to:

- **Divide Taiwan's society:** By exacerbating existing societal cleavages, China weakens Taiwan's collective will and its ability to pass legislation that would strengthen its defenses. This division also erodes public satisfaction with democracy, feeding into the second objective[3].

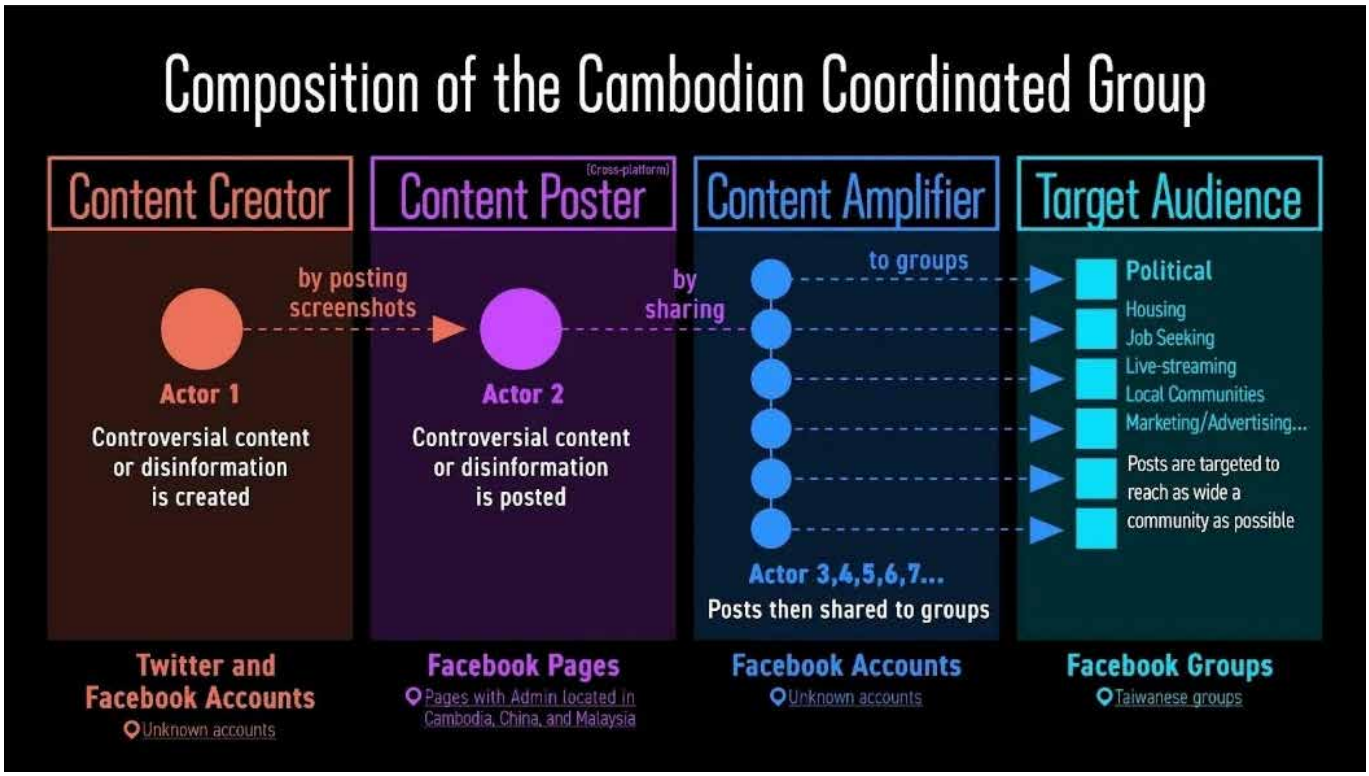


Figure 1 Chinese Information Attack

- **Degrade the pro-Taiwan political camp:** China consistently targets the pro-Taiwan political camp, often portraying them as "provoking China" and thereby harming ordinary citizens through economic or military repercussions [4].

To achieve these deep narratives, China employs a steady stream of "granular stories" as evidence. Rather than directly stating "the government is corrupt," the strategy involves a constant flow of specific, often fabricated or exaggerated, stories about corruption, such as alleged malfeasance in importing toxic eggs or unsafe vaccines.[5] These formulaic story patterns become "propaganda tropes" that, over time, are designed to embed China's core messages into Taiwan's public consciousness.

For example, to promote economic opportunities, specific stories of Taiwanese businesspeople or artists succeeding in the Chinese market are highlighted. To portray Taiwan's military as inept, any new equipment failures are amplified.

China's influence extends beyond mere messaging; it employs "hybrid" elements, integrating information warfare with other tools of state power. Examples include:

- **Cutting undersea internet cables:** This creates strategic anxiety, demonstrating China's ability to isolate Taiwan[6].
- **Attempted assassination of Taiwan's VP in Prague:** This one failed, but suppose they succeeded? The message would have been that China is all-powerful and can even murder Taiwan's vice president when visiting an ally in Europe.[7]
- **Military drills and economic manipulation:** These actions[8] are presented as responses to perceived "provocations" by Taiwan, aiming to create fear and economic hardship[9], thus tying back to the narrative that the pro-Taiwan political camp is "provoking China."
- **Hacking:** During moments of heightened tension, such as Pelosi's visit, 7-11 displays were hacked to induce strategic anxiety.[10]

The infrastructure supporting these campaigns is vast and sophisticated, leveraging both official channels (diplomats, state media) and covert state-linked accounts that mimic independent voices. Increasingly, China relies on local actors within Taiwan to seed and amplify its messages. These local actors can be genuinely aligned with China's interests, entrepreneurial individuals seeking to monetize attention, or direct proxies receiving funding and orders. This approach enhances effectiveness, as local voices are more trusted, and obscures Beijing's involvement, allowing it to claim these are "internal issues."

A concerning development is the "industrialization of information manipulation" through private "influence for hire" services. Companies like GoLaxy reportedly use AI to collect social media data, build psychological profiles of citizens, and deploy AI-driven fake accounts for targeted persuasion.[11] Furthermore, there's an observed overlap between financial scamming networks and China's information warfare infrastructure, with many operations traced back to organized crime hotbeds linked to China[12].

The impact of platforms like TikTok is particularly alarming. Its algorithmic recommendation engine, controlled by the Chinese government, is observed to correlate with an increased belief in China's deep narratives among Taiwanese users, regardless of their existing political preferences. This suggests a systemic manipulation of the information environment disproportionately affecting younger generations,

potentially reshaping Taiwan's future political landscape.[13]

Beyond Taiwan: A Global Playbook

China's information warfare is not confined to Taiwan; it's a global playbook with elements applied to various countries and regions[14].

A strategic interest that crosses international boundaries is image management. China has employed similar propaganda tropes to whitewash human rights abuses in Hong Kong and East Turkestan. The full spectrum of the PRC's infrastructures of information manipulation are deployed to spread propaganda tropes such as "Happy Uyghurs" that presents a Potemkin village of smiling, dancing Uyghurs in traditional dress to counter international criticism and justify Beijing's policies [15].

At a global level, China aims to undermine faith in democracy as a system, and to drive divisions within societies that serve their strategic interests. Similar operations have been observed to divide target audiences within and drive wedges between other countries:

- **Lithuania:** GoLaxy has reportedly been involved in operations aimed at driving division between Taiwan and Lithuania at the international level[16].
- **India:** An astroturf campaign spread a narrative claiming that allowing Indian workers into Taiwan would lead to a sexual assault epidemic, gaining traction among Indian influencers and portraying Taiwan's society as racist to Indian audiences[17]. In the Indian information space, China pushes narratives attacking the Indian government, degrading the image of Prime Minister Modi, stoking divisions in India's northern border regions, and attacking perceptions of India's democracy with polarizing content[18].
- **Philippines:** China amplifies internal divisions in the Philippines, deploying state media and inauthentic social media assets to spread disinformation, such as a recent deepfake of President Marcos purportedly using drugs[19].
- **United States:** During the 2024 US election, a massive cross-platform network of inauthentic social media accounts attributed to China's Ministry of Public Security was observed amplifying domestic political divides[20].

This demonstrates that China's strategy of exploiting and amplifying polarization is a pervasive tactic used to achieve its geopolitical objectives across diverse contexts.

Beyond China's direct information warfare against other nations, there are also many signs of strategic and tactical alignment with other authoritarian states such as Russia, Iran, and North Korea in the information domain[21].

The Path Forward: Safeguarding Democracy in the Digital Age

The challenges posed by sophisticated information warfare and online polarization demand a robust and multi-faceted response.

First, enhanced **monitoring and reporting** are crucial. A comprehensive understanding of China's hybrid cognitive warfare infrastructure, its methods, and its key actors is necessary for situational awareness and to gather objective evidence for future actions.

Second, **strategic communications** must be prioritized. This doesn't mean engaging in information manipulation, but rather empowering pro-democratic com-

Figure 2 A model for Foreign Information Manipulation interference (FIMI) Resilience – Building FIMI Resilience Democracy

municators, influencers, and content creators to defend democratic values and engage key audiences with evidence-based narratives. Given the vast resources China invests, strategic targeting of audiences and messages is paramount.

Third, **policy development** is essential. Laws and regulations need to be adapted to disrupt China's infrastructure of information manipulation. The overlap between financial scamming and information warfare infrastructure presents an opportunity to develop legislation, perhaps using consumer fraud laws, to prosecute fake social media accounts and the entities behind them.

Fourth, **coalition building** is vital. Democracies are out-resourced and often out-coordinated by authoritarian regimes. By sharing intelligence, resources, and aligning on strategic communications, democratic nations can collectively counter shared threats, such as resisting economic warfare and military adventurism. This is not just a high-minded ideal but a matter of collective self-interest.

Finally, it is crucial to recognize that this is fundamentally a political problem. While information warfare operates in the digital realm, its effectiveness is often amplified by real-world grievances. As long as democracy is perceived as failing its citizens, efforts to counter disinformation will only offer short-term solutions. Pro-democratic politicians, supported by civil society, must actively address people's legitimate concerns and solve societal problems to build resilience against external manipulation. Addressing these foundational issues in society is the most effective long-term defence against the corrosive effects of online polarization and foreign influence.

AUTHORS:

FREDDY LIM

CURRENT POSITIONS

Ambassador,
Taiwan Representative Office
in Finland (since July 2025)
Lead Vocalist, CHTHONIC
(since 1996)

PREVIOUS POSITIONS

Member of Parliament,
Taiwan (2016–2024)
Chair, Amnesty International
Taiwan (2010–2014)

Ttcat

Co-founder and CEO,
Doublethink Lab

Wu Min-Hsuan (Ttcat) is the co-founder and CEO of Doublethink Lab, a Taiwan-based organization founded in 2019 to strengthen the information space against manipulation and online threats. He is a lead director of the China Index and coordinator of the China In The World network, which connects experts and organizations to study how influence campaigns operate globally.

In the Indo-Pacific, Ttcat leads projects on Foreign Information Manipulation and Interference (FIMI), supporting local partners to track emerging narratives and their spread. His team also conducts polling and survey research to understand how these narratives shape public opinion and to build strategic responses for democratic resilience.

TIM

Tim Niven,
Deputy CEO
of Doublethink Lab

Tim Niven serves as Deputy CEO at Doublethink Lab. A computational social scientist by training, Tim applies artificial intelligence to the monitoring and analysis of foreign information manipulation and interference. Tim has been with Doublethink Lab researching China's information manipulation strategy and tactics for five years and has published work on propaganda whitewashing human rights abuses in Hong Kong and East Turkestan, PRC laundering of Russian propaganda, and China's information warfare targeting Taiwan.

REFERENCES/SOURCES

1 Misinformation exploits outrage to spread online https://pubmed.ncbi.nlm.nih.gov/39607912/

2 2024 Global research project Varieties of Democracy, Department of Political Science at the University of Gothenburg. https://www.taipeitimes.com/News/taiwan/archives/2024/03/25/2003815440

3 Journal of Democracy: How Taiwan Should Combat China's Information War

https://www.journalofdemocracy.org/online-exclusive/how-taiwan-should-combat-chinas-information-war/

4 Journal of Democracy: Combating Beijing's Sharp Power: Taiwan's Democracy Under Fire

https://www.journalofdemocracy.org/articles/combating-beijings-sharp-power-taiwans-democracy-under-fire/

5 Doublethink Lab: Artificial Multiverse: Foreign Information Manipulation and Interference in Taiwan's 2024 National Elections

https://medium.com/doublethinklab/artificial-multiverse-foreign-information-manipulation-and-interference-in-taiwans-2024-national-f3e22ac95fe7

6 Global Taiwan Institute: China's Undersea Cable Sabotage and Taiwan's Digital Vulnerabilities https://globaltaiwan.org/2025/06/taiwans-digital-vulnerabilities

7 The Guardian: China 'planned car collision' during Taiwan vice-president's visit to Prague https://www.theguardian.com/world/2025/jun/28/taiwan-vice-president-undeterred-after-czech-reports-of-alleged-chinese-car-collision-plot

8 Reuters: China launches 'punishment' war games around Taiwan https://www.reuters.com/world/asia-pacific/china-starts-military-drills-around-taiwan-days-after-new-president-takes-office-2024-05-23/#:~:text=BEIJING%2FTAIPEI%2C%20May%2023%20%28Reuters%29%20,te

9 Reuters: China threatens more trade sanctions on Taiwan as election nears https://www.reuters.com/world/asia-pacific/china-threatens-more-trade-sanctions-taiwan-election-nears-2023-12-27/

10 Taipei Times: PELOSI'S VISIT: Digital displays attacking Pelosi were hacked: CIB https://www.taipeitimes.com/News/taiwan/archives/2022/08/04/2003782956

11 NYT: The Era of A.I. Propaganda Has Arrived, and America Must Act https://www.nytimes.com/2025/08/05/opinion/china-ai-propaganda.html

12 FDD: Nip the Bots in the Bud: Proactively Taking Down and Preventing the Creation of Inauthentic Social Media Entities https://www.fdd.org/wp-content/uploads/2024/08/fdd-memo-nip-the-bots-in-the-bud-proactively-taking-down-and-preventing-the-creation-of-inauthentic-social-media-entities.pdf#:~:text=Te%20Foundation%20for%20Defense%20of,malicious%20activity%20on%20social%20media

13 Doublethink Lab: From Social Entertainment to United Front Narratives: TikTok's Role and Reshaping of Taiwan's Socio-Psychological Defenses https://medium.com/doublethinklab/from-social-entertainment-to-united-front-narratives-tiktoks-role-and-reshaping-of-taiwan-s-1f6d0b5bc1b0

14 Doublethink Lab: China Index 2024: Mapping PRC Influence Across 101 Countries — Full Report https://medium.com/doublethinklab/china-index-2024-mapping-prc-influence-across-101-countries-full-report-6adc37562677

15 Doublethink Lab: Reports: Whitewashing Hong Kong and East Turkistan https://medium.com/doublethinklab/reports-whitewashing-hong-kong-and-east-turkistan-c00dfc423dc5

16 Vanderbilt University Golaxy Paper: https://www.vanderbilt.edu/national-security/wicked-problems-lab/golaxy/

17 NDTV: Opinion: Racism, Disinformation Cast Shadow On India-Taiwan Cooperation https://www.ndtv.com/opinion/racism-disinformation-cast-shadow-on-india-taiwan-cooperation-4579209

18 ASPI: Beijing's online influence operations along the India–China border https://www.aspistrategist.org.au/beijings-online-influence-operations-along-the-india-china-border/

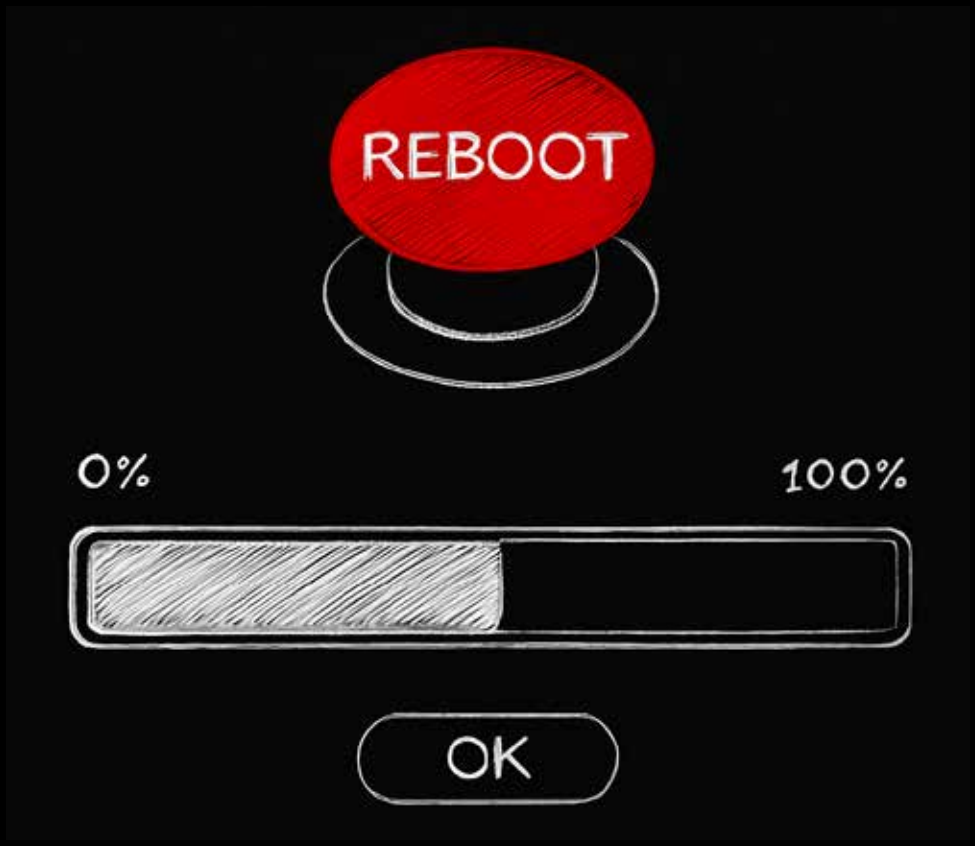
19 ASPI: China's high stakes and deepfakes in the Philippines https://www.aspistrategist.org.au/chinas-high-stakes-and-deepfakes-in-the-philippines/

20 NYT: China's Advancing Efforts to Influence the U.S. Election Raise Alarms https://www.nytimes.com/2024/04/01/business/media/china-online-disinformation-us-election.html

21 Belfer Center for Science and International Affairs, Harvard Kennedy School: A Next Generation National Information Operations Strategy and Architecture https://www.belfercenter.org/publication/next-generation-national-information-operations-strategy-and-architecture

IGA REBOOT

Do you really know who can access your systems?



With Seafront™ IGA, you always know – access is automatic, secure, and audit-ready.

Book a free consultation:
sales@haidion.com
www.seafrontidm.com

Haidion | Seafront

FINNISH SERVICE

JOONAS JOKINEN

Reinventing Identity and Access Management – How to Support Business Growth Securely

Renewing an organization's Identity and Access Management (IAM) solution is no small decision. Yet IAM forms the very foundation of the entire digital environment: it governs who can access which data and systems. Its reach can be surprisingly broad from employees to external partners, and all the way to automation and machine accounts. No wonder the mere thought of replacing the system can cause cold sweat. But why is now the right time to stop and reconsider the relevance of your IAM solution and what can it bring to the business?

When Does IAM Need Renewal?

Many organizations only recognize the need for an IAM system once daily work starts becoming inefficient. If HR sends new employee information to IT by email, and IT then manually creates accounts and passwords, that is far from modern automation. The same inefficiency is visible to end users: if access rights must be requested via email and every application requires a separate login, time and patience are wasted while security risks grow.

Other signs of outdated IAM include obsolete technology, poor integrations, clunky user interfaces, or security that no longer meets current requirements. Often, projects are launched only under external pressure, say, after an audit finding or a security incident. In such cases, decisions may be rushed without a clear strategy.

What Does Modern IAM Deliver?

Next-generation IAM systems are not just back-end technical tools. They bring organizations three key benefits: security, a better user experience, and efficiency.

From a security standpoint, IAM is a critical line of defense. A system implemented years ago may no longer meet today's requirements, leaving the organization vulnerable. In addition, legislation and regulations such as GDPR and NIS2 require controlled access management and transparency.

From a user experience perspective, a modern solution can be almost invisible: employees receive the right access immediately upon starting their job, log in once, and seamlessly use all necessary applications without friction. For administrators, the system is easy to manage without lengthy and costly training. When IAM is integrated with HR, service management, and business applications, access rights are created automatically and remain up to date throughout the entire employee lifecycle. This frees up time from manual tasks for actual business development.

Problems often arise when organizations focus too much on individual features during selection. Later, during implementation, they discover the solution is more complex and expensive to maintain than expected. That's why the choice should emphasize business value and long-term goals—not just a checklist of technical requirements.

How to Succeed in Renewal?

Once the need for renewal is identified, organizations should proceed step by step. The first step is to assess the current state: how are identities managed today, and does the system meet regulatory requirements? Next comes defining the IAM strategy—what are the goals, such as stronger security, better efficiency, or improved user experience? The final step is a realistic set of requirements to ensure the system supports the business without becoming overly complex.

Success requires involving all key stakeholders from the very beginning—not just IT, but also business units, HR, security, and audit. When perspectives are combined, the initiative becomes not just a technical project but a strategic undertaking.

Looking Ahead

Identity and access management is constantly evolving. New requirements emerge as digital environments grow more complex from stricter regulations to new types of identities. That's why it is essential to choose a partner who actively develops their IAM services and ensures the solution meets both today's needs and tomorrow's challenges.

Competitive Advantage, Not a Cost Center

Renewing your IAM system is not merely an IT project. It is a strategic investment that improves security, streamlines processes, and simplifies daily work. Done right, identity management is not just an expense—it is a competitive advantage.

Is your organization ready to take the next step?

AUTHOR:

For more than a decade, Joonas Jokinen has been helping organizations make their digital services secure, efficient, and easy to use through identity and access management (IAM). Today, he brings his expertise to Haidion as an IAM Architect, where he continues to bridge the gap between technology and business needs.

JOONAS JOKINEN

ALEXEY BOLTUNOV

The Data Iceberg: Protecting What You Don't See in Times of Instability

Today, political conflicts and geopolitical tensions are reshaping the landscape of cyber threats[1]. Critical infrastructure—energy, healthcare, defense, supply chains—has become a prime target[2]. Cyberattacks are no longer only about financial gain. They're also about disruption, influence and power.

The Rise of State-Sponsored Cyber Operations

Whereas cyberattacks were typically associated with hackers, now there's the emergence of state-sponsored and politically motivated[3] actors that have the potential to access far greater resources than your everyday cybercriminals. This, in turn, allows their operations to be highly professional, carefully researched and precise.

Instead of broad and largely opportunistic campaigns, these kinds of attackers are able to conduct localized, organization-specific missions. For example, *spear phishing*[4] and *customized malware*[5] can be created to exploit the smallest traces of data that may be left behind on a person of interest's system.

More Regulations & Compliance Demands

Governments are responding to advanced cyberattacks with stricter cybersecurity regulations, such as NIS2[6] in the EU and the CCPA[7] in California. These laws provide a valuable foundation by empha-

sizing accountability and pushing organizations to strengthen their defenses. Yet most compliance frameworks primarily focus on visible data, such as documents, emails and media files. But under the surface lies a much larger mass of hidden and residual data that often remains overlooked.

The Data Iceberg: A Hidden Security Problem

To comply with compliance regulations, most organizations understandably build their security strategies around visible data. They protect files that employees handle every day, such as spreadsheets, contracts and email attachments. But, in addition to visible data, there's hidden layers of system data that typically remains unaddressed. This kind of invisible data includes cache files, temporary files, metadata and residual data that quietly accumulate in the background.

Only dealing with visible data creates an illusion of security. Organizations may feel safe after meeting regulatory requirements, but, in reality the majority of their data is invisible and still exposed. For advanced attackers, that hidden data is a goldmine.

You can think of the total amount of data that needs protecting within an organization as an iceberg. The visible files above the waterline only make up the tip, but beneath the surface lies a much larger body of invisible and residual data. It's in this space that attackers often go looking.

Above the Waterline: Visible Data (10-25%)

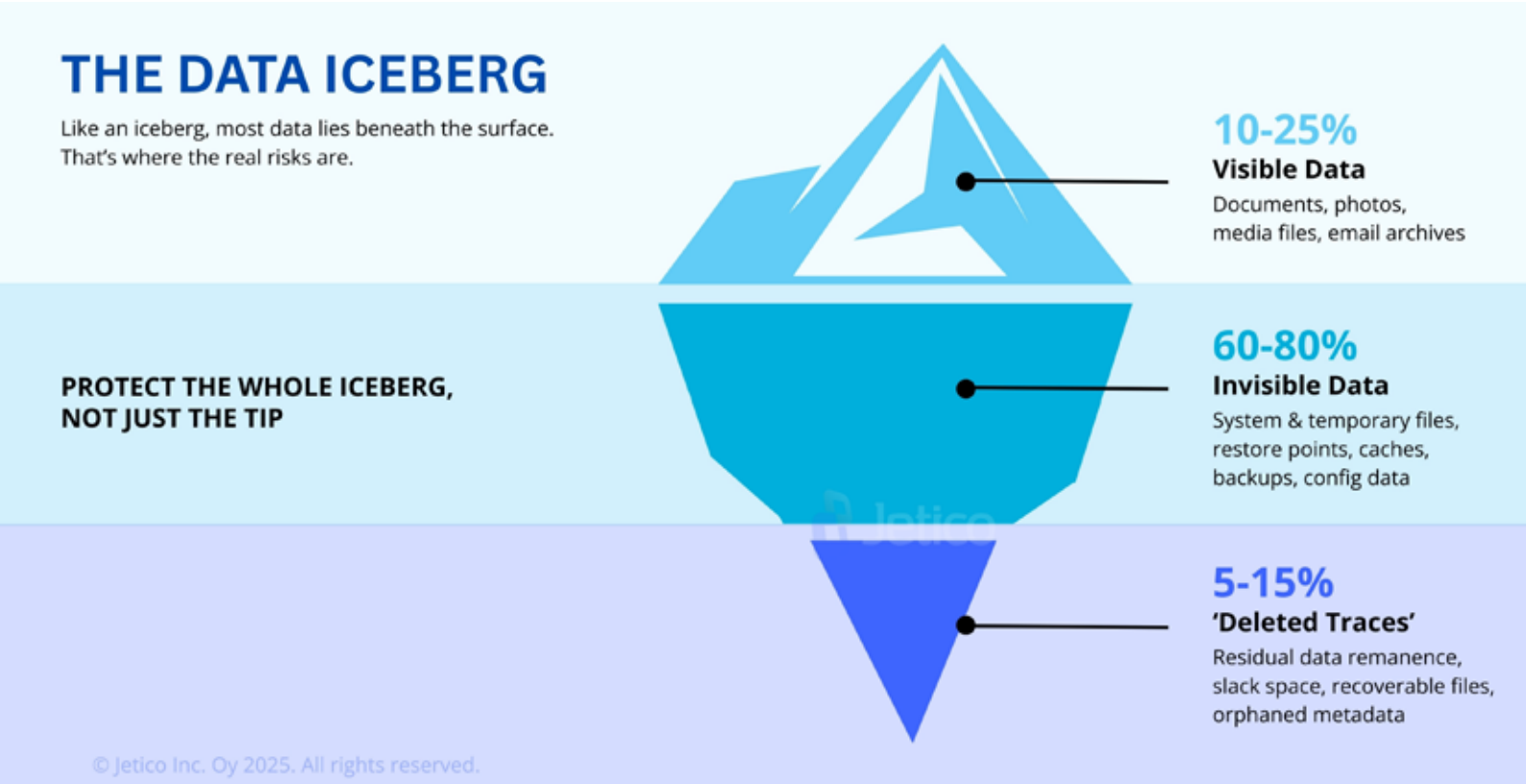
This is the information that most people think of when discussing data protection, mainly consisting of user-created files like documents, spreadsheets, PDFs, photos, media and email archives. Within an organization's data iceberg, the visible data is likely to be actively managed and regularly backed up.

Below the Waterline: Invisible Data (60-80%)

Invisible data refers to the type of information residing on organizational systems that is not typically modified or even thought of by users. This larger part of the iceberg includes:

- System restore points
- Shadow copies, i.e. backup copies of data that remain after being deleted by normal means
- Temporary files, such as caches and memory dumps
- Application caches, which contain fragments of data that users are working with
- Invisible backups and redundant copies

You can think of this midsection of the iceberg as the shadow layer. It's essential for system maintenance,



but often hidden to standard security practices and liable for attackers to target.

The Deepest Layer: Traces of Deleted Files (5-15%)

The final stratum of the data iceberg is reserved for the information that remains after files are "deleted" by normal means, even those that were "permanently deleted" on Windows[8] to bypass the Recycle Bin. Doing so only removes references to the files in question, leaving the file data and related information intact in various places on organizational systems. The actual data will remain until its overwritten, which can take weeks or even months.

This kind of residual data, otherwise known as data remanence, can appear in several forms:

- Residual data remanence
- File slack space
- Recoverable files
- Orphaned metadata in indices, journals or registry hives

Unbeknown to organizations, cybercriminals using forensic tools can often recover gigabytes of this type of data.

The Risks of Invisible and Residual Data

As explained in the above section, "deleting" a file by regular means doesn't make it disappear. *Residual traces often remain*[9] and can be pieced back together by hackers to reconstruct documents, communications or credentials. Similarly, invisible data like *shadow copies*[10] and temporary files[11] are likely to reveal snapshots of user activity that can expose confidential business content. These hidden layers account for around 60–80% of potentially sensitive data, which is often left unprotected by organizations.

While this is risky in any context, the consequences are amplified in today's geopolitical climate. Here's 3 reasons why:

- **The Value of Intelligence:** It only takes a small fragment of invisible data to provide adversaries with insights into strategies, infrastructure or operations. What's more, state-sponsored actors have the resources to extract and weaponize these traces.
- **Erosion of Trust:** Partners, clients and allies expect airtight defenses. A leak of invisible data undermines credibility and weakens cooperation.
- **Operational Disadvantage:** Exposed system data can reveal activity patterns or vulnerabilities. In times of conflict, this intelligence may allow adversaries to anticipate responses and exploit weaknesses.

Protecting the Full Data Cycle

So, how should you protect the data iceberg in its totality to avoid the risks outlined above? Well, you can start by thinking about and protecting data in complete protection cycles. This means safeguarding data from creation, through daily use and, finally, with proper end-of-life disposal. Without closing this loop, invisible traces remain exposed, waiting to be exploited.

Bridging the Gap

Most organizations already recognize the importance of securing visible data and sanitizing endpoints when they're no longer in use. Yet between those two states lies a wide-open gap composed of invisible data and deleted traces. This is exactly where state-sponsored attackers thrive. Traditional blacklist approaches, i.e. blocking only what's known, fall short. To cover the gap, organizations need to shift toward a *whitelist mindset*[12]. This means thinking in terms of only allowing trusted applications and processes, helping to secure both the visible and invisible layers of data.

The Role of Data Wiping

One essential technique in closing this gap is data wiping. While encryption safeguards stored information, data wiping ensures that deleted information is truly gone. Unlike deleting files by regular means, which leaves traces behind in various places, data sanitization overwrites information so it cannot be recovered even with the help of forensic tools.

To further level up your security, advanced data wiping techniques can also be used. Certain solutions allow organizations to not only remove individual files, but also automatically target invisible files created and discarded by the operating system and applications. This results in temporary files, shadow copies and other kinds of data remanence being securely erased before they ever become a liability.

Closing the Loop with Jetico

For more than 30 years, Jetico has helped governments, defense agencies and enterprises secure sensitive information against everyday risks and advanced threats. Our solutions are designed to address the critical gap between encryption and endpoint sanitization—covering the entire data iceberg, from the visible tip to the hidden layers.

Here's how we help organizations protect the full data cycle:

- **Encryption:** *BestCrypt*[13] protects visible, user-facing files like docu-

ments and media that regulations require organizations to secure.

- **Secure erase:** *BCWipe*[14] forensically removes data remanence, addressing the blind spot left by most regulations. Once a government-grade need, data sanitization is now essential for all organizations.
- **Data discovery:** *Search*[15] helps organizations reveal where invisible or vulnerable data resides, allowing encryption and data wiping to be applied systematically.
- **Granular access control:** *BestCrypt Data Shelter*[16] ensures sensitive files can only be accessed by authorized applications, providing a whitelist approach that minimizes exposure points and prevents data leaking through untrusted processes.

Protect the Whole Iceberg, Not Just the Tip

Invisible and residual data may be out of sight, but it shouldn't be out of mind. As geopolitical tensions rise and attackers grow more sophisticated, the hidden bulk of the data iceberg is exactly where the greatest risks lie. Ignoring it creates blind spots that compliance regulations alone cannot close. By addressing the entire data lifecycle and employing a whitelist mindset, organizations can reduce the risks of data leaks, compliance failures and reputational damage. The result? Peace of mind through resilience.

REFERENCES/SOURCES

1 World Economic Forum. Global Cybersecurity Outlook 2025: A Complex Cyberspace. https://www.weforum.org/stories/2025/01/global-cybersecurity-outlook-complex-cyberspace-2025/

2 Reuters. Singapore says cyber-espionage group targeting critical infrastructure. https://www.reuters.com/world/china/singapore-says-cyber-espionage-group-targeting-critical-infrastructure-2025-07-18/

3 F-Secure. What are state-sponsored cyber attacks? https://www.f-secure.com/en/articles/what-are-state-sponsored-cyber-attacks

4 IBM. Spear Phishing. https://www.ibm.com/think/topics/spear-phishing

5 Dark Reading. Customized Malware: Confronting an Invisible Threat. https://www.darkreading.com/vulnerabilities-threats/customized-malware-confronting-an-invisible-threat

6 European Union. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). https://eur-lex.europa.eu/eli/dir/2022/2555

7 California Office of the Attorney General. California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa

8 Microsoft Support. How to bypass the Recycle Bin when deleting files. https://support.microsoft.com/en-us/topic/how-to-bypass-the-recycle-bin-when-deleting-files-36aa9c63-c12a-988f-43c4-e4347e2b2825

9 Jetico. What is Data Remanence & How to Remove It in 5 Easy Steps. https://jetico.com/blog/what-data-remanence-how-remove-it-5-easy-steps/

10 Jetico. Unprotected Shadow Copies – How to Delete Them in Windows 10/11. https://jetico.com/blog/unprotected-shadow-copies-how-delete-them-windows-1011/

11 Jetico. What Are TMP Files & How Should I Delete Them? https://jetico.com/blog/what-are -tmp-files-how-should-i-delete-them/

12 CSO Online. Whitelisting explained: How it works and where it fits in a security program. https://www.csoonline.com/article/569493/whitelisting-explained-how-it-works-and-where-it-fits-in-a-security-program.html

13 Jetico: Data Encryption https://jetico.com/data-encryption/

14 Jetico: Data Wiping https://jetico.com/data-wiping/

15 Jetico: Sensitive Data Discovery Tool Integrated with Jetico's Wiping Solution Delivers First-Ever Combined Approach for Effortless Data Management https://jetico.com/news/sensitive-data-discovery-tool-integrated-jeticos-wiping-solution-delivers-first-ever-combined/

16 Jetico: BestCrypt Data Shelter https://jetico.com/free-security-tools/data-in-use-protection-with-bestcrypt-data-shelter/

AUTHOR:

Alexey Boltunov has served as Jetico's Chief Operating Officer (COO) since 2023, bringing with him over a decade of experience that combines technical expertise with strategic business acumen. Aligning innovation with business goals, Boltunov ensures company strategies are seamlessly implemented into daily operations. Boltunov's hands-on leadership and deep understanding of technology and customer behavior continue to drive Jetico's success in delivering user-focused, cutting-edge data protection solutions.

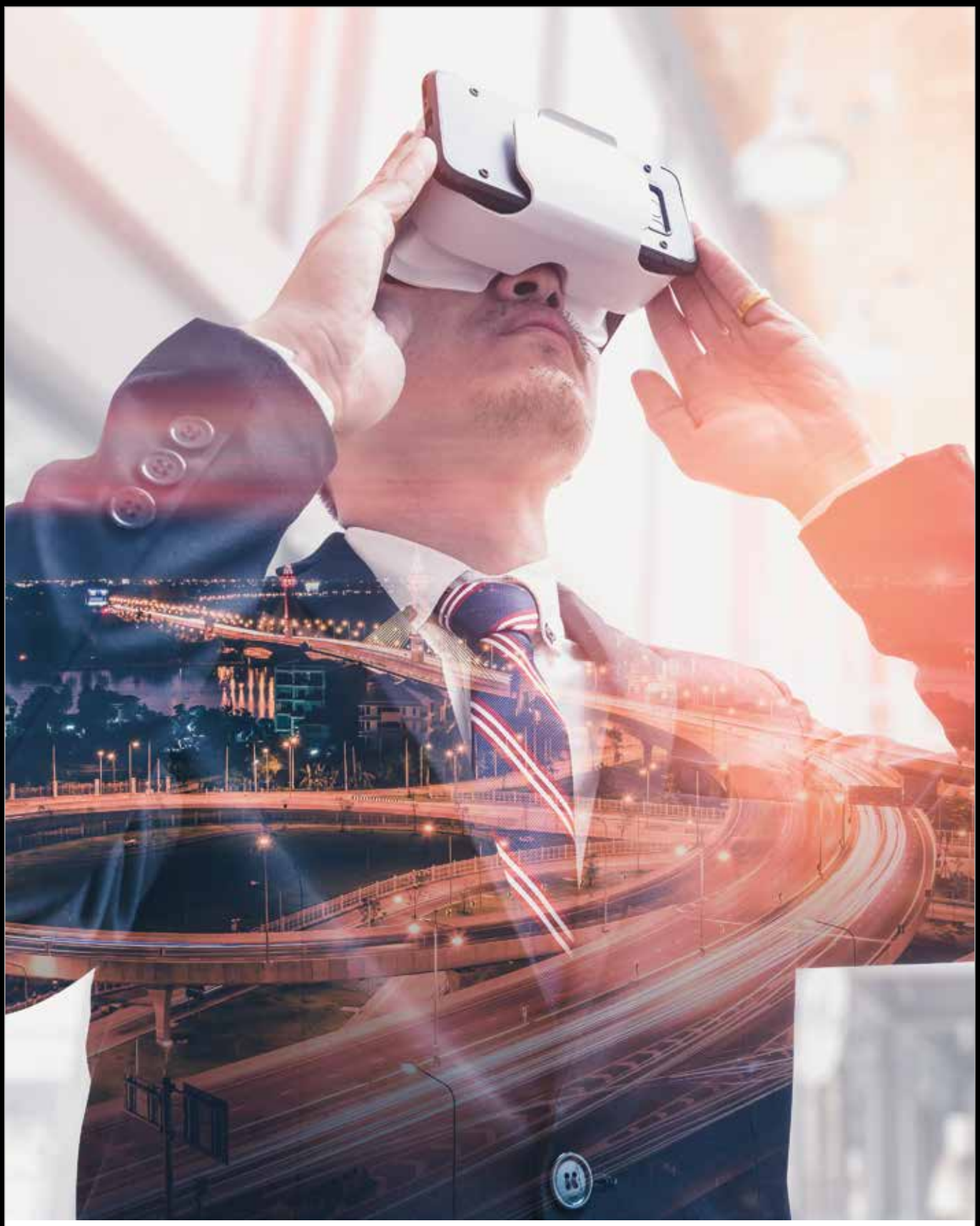
ALEXEY BOLTUNOV

Cyberwatch Finland

MONTHLY REVIEW

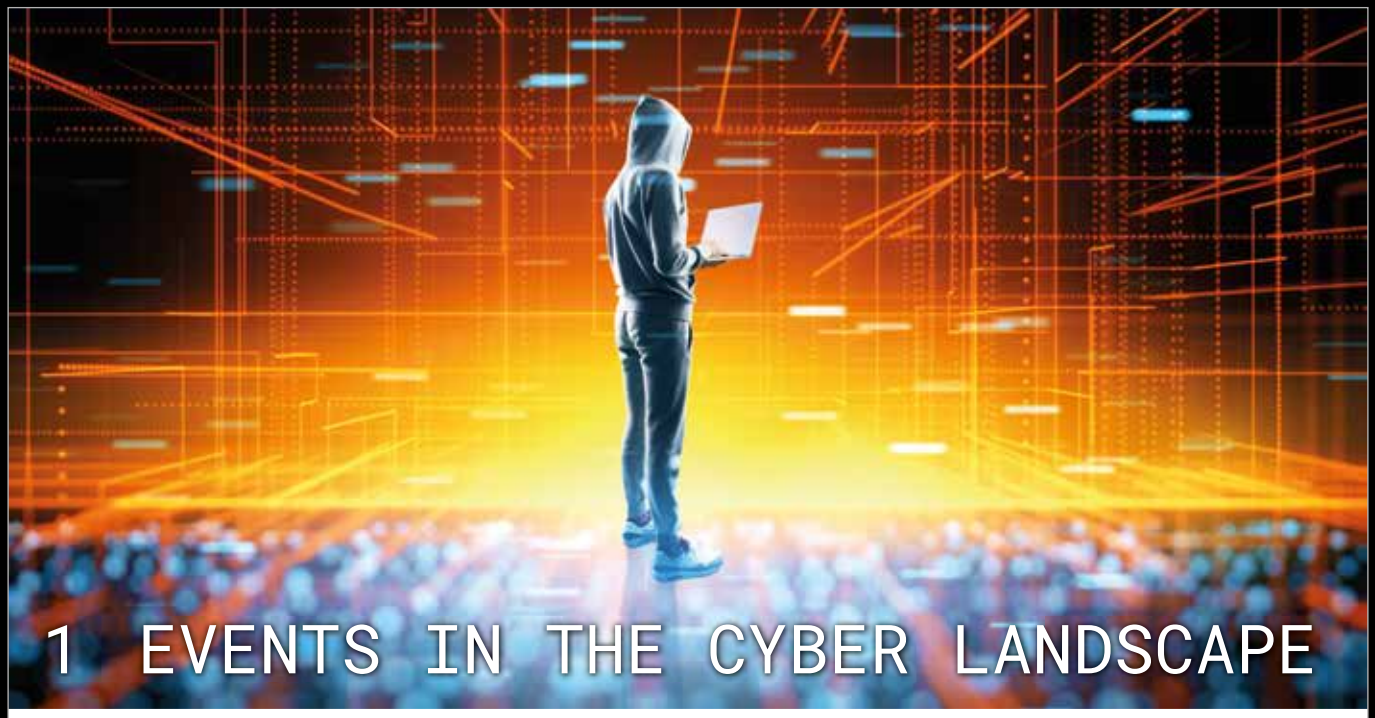
OCTOBER/2025

Cybersecurity is Built by Small Actions and Management of Large Concepts



In this review

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



1 EVENTS IN THE CYBER LANDSCAPE

In September, Moldova's parliamentary elections received a lot of international attention. In the elections, the pro-EU Action and Solidarity Party (PAS), which was in power, faced off against the pro-Russian Patriotic Electoral Bloc (PEB). The elections ended with a victory for the PAS, even though Russia aggressively and transparently tried to influence the result through cyber and hybrid means. Although the result was good from a Western perspective, and it has been seen as a sign of Moldova's reunification and the weakening of Russia's influence, it should not be seen as a mere failure for Russia, as it achieved at least some of its goals. The most important of these is the attempt to increase the internal divisions within the target country and escalate the confrontation. In Moldova, this was related to the rights of the Transnistrian region and the people living there. Transnistria is a Russian-occupied region in Moldova that, with the help of Russian support, is de facto independent, although officially still belongs to Moldova. According to Russian sources, Moldova tried to prevent Transnistrian residents from voting and limit their rights. The claims were based on the fact that polling stations could not be safely set up in Transnistria, so residents usually had to travel a few kilometres to the Moldovan side to vote. At the same time, media linked to Russia shared news of a likely takeover of Moldova by NATO troops if the PAS wins the elections. Instead of an outright election victory, Russia is seeking to increase the confrontation within Moldova between those who are pro-EU and pro-NATO and those who support Russia, and these efforts will certainly continue regardless of the outcome of the elections. Just before the elections, thousands of fake accounts, mostly maintained by artificial intelligence, were spotted on social media, sharing and repeating Russian narratives. For example, the video service Youtube announced that it had been forced to remove more than a thousand channels specifically for sharing fake content related to the Moldovan elections. A few days before the elections, Russian hacker groups also tried to take down voting systems with cyberattacks, but these were mostly successfully repelled.

In September, a major information leak was also revealed in Sweden. The actual data breach took place at the end of August and was revealed in the first week of September, when the database of Miljödata, which provides services to the Swedish municipal sector, was published on the dark web. Behind the attack was a relatively unknown ransomware actor called Datacarry, which has already claimed well over a dozen victims. Ransomware groups rarely publish entire databases except in cases where the demands have not been agreed to or negotiations have failed, so this can be assumed to have happened in the case of Miljödata. In any case, the personal data of almost a million Swedes is now openly available on the dark web, which is likely to lead to identity theft and phishing attempts against them and their loved ones. The case highlights the contradiction that comes with extortion cases: Criminals should not be paid or their demands granted, and that rarely leads to anything positive. However, non-payment can lead to situations like the one we have now observed and, at least in the case of Miljödata, also to reputational damage and accusations. At the moment, it is not known whether the attack could have been prevented, and what kind of level of information security Miljödata has. The answer to this will certainly be sought for a long time to come. As a lesson learned from the situation, it can be said that it is much cheaper to take care of information security so that you never get attacked than to consider between several bad options when the databases are already in the possession of criminals.

2 IN THE SPOTLIGHT

2.1 The current state of spyware

In the beginning of September, the Atlantic Council published a follow-up to its report on spyware from 2024. This time, their focus was on tracking down the partners working with spyware companies to obscure the connections between vendors, suppliers and buyers as well as reflecting on the trends identified in the first report. The report illustrates how US investment in spyware has rapidly increased, despite the fact that the US government is trying to fight against spyware with more and more legislation. Consequently, American money is now financing the means to spy on Americans. For the first time ever, US investment has surpassed the Israeli one, and not by a small margin.

The role of partners was found to be much more important than previously thought. They are used to deliberately obfuscate the connections between vendors and buyers to make it harder to discover what is being sold and to whom. Despite their significance, they are currently not being targeted in any way with legislation concerning spyware. That might prove to be an oversight in the future.

Israel, India and Italy are the largest spyware producers in the world but, perhaps more interestingly, new entities include locations such as Malaysia and Japan. It seems that although the US is emerging as the main source of investment, the market itself is becoming more global and diverse. It is worth noting, that if governments such as the US truly wanted to take a strong stance against spyware, they would not allow their citizens to invest in it. That said, if the US investment was to be cut off right now, it would not completely stop the proliferation of spyware.

Meanwhile, Apple just introduced a new security feature it proclaims is going to effectively mitigate the threat of spyware: Memory Integrity Enforcement (MIE). It works in tandem with the Enhanced Memory Tagging Extension (EMTE), which is an upgrade to a previous system dating back to 2019. MIE is the software feature that enables EMTE to work without massively slowing down the device, but it also improves the safety of devices that do not have EMTE, which is currently only included in the newest iPhone 17 series and iPhone Air. Without going into too much technical detail, EMTE is a hardware feature in the memory of Apple devices that attempts to counter the memory corruption bugs very commonly exploited by spyware.

Previously, no countermeasure existed against them, but now not only the newest Apple devices, but hopefully soon all others as well are finally going to be resistant. That is because Apple has made the EMTE feature publicly available to speed up industry-wide implementation. Only time will tell how much of an impact these are going to really have on spyware, but at the very least attacks should now become more difficult and expensive.

2.2 The diverse threats to aviation in Europe

European aviation has been under constant threat in September. Recent headlines have been dominated by news of drone activity near Danish airports. Before that, a cyberattack against a check-in system used on many airports throughout Europe resulted in serious delays and cancellations of flights for more than a week. Even before that, Russian drones flew into Poland, forcing the local government to close parts of its airspace for hours. When looking at the situation as a whole, it seems like European aviation in general is currently being systematically harassed. This is further backed by a report by the French aerospace company Thales, which states that cyberattacks against the aerospace industry have increased by a staggering 600% over the past year.

It is likely not possible to prove that all of these incidents are connected or mutually coordinated, but there is a very high possibility at least some of them are. The main suspect, as usual, is Russia. The country suffered a serious hit to its own aviation industry during the summer, when hackers managed to cripple the systems of Aeroflot, resulting in massive amounts of delays and cancellations of flights throughout the country. Russia might be trying to get revenge by targeting European aviation in return, and it could also serve as a way to divert attention away from the problems Aeroflot was facing earlier. This way the Russian population could be persuaded that it was not in fact domestic incompetence that ruined their vacation plans, but rather an international problem that the government could not have prevented.

Another reason for Russia to execute these kinds of operations is to bait a strong response out of the West. Then it could show its citizens that the claims of the West being at war with Russia are in fact true, and the West is just lying about the matter. Both of these motives are tightly linked to information warfare. As seen throughout the war in Ukraine, that is often the case with Russian cyber operations. In this case, they are primarily intended to influence a domestic audience, but it is an undeniable truth that they have had an impact in the West as well. The cyberattack against the check-in systems was directed at a single service provider and still managed to cause serious and widespread disruptions. Both the Europeans and also the threat actors must be thinking about the possibility of scaling up. What would happen if multiple such attacks were to be coordinated and combined with say, unidentified drones flying near airports?

2.3 The AI boom offers opportunities for criminals

With the rise of artificial intelligence and the advancement of technology, the number of applications utilising it has grown exponentially. As people come up with more and more creative uses for artificial intelligence, these naturally need their own applications, and as new uses are constantly being invented, the number of new applications is also constantly increasing. Threat actors have also noticed this and are taking advantage of the boom by developing their own ”artificial intelligence applications” that are actually intended to spread spyware or data-gathering malware.

In September, Japanese security house Trend Micro announced that it had detected a wide wave of applications like this, which it called EvilAI. In practice, the researchers observed dozens of applications that emerged almost simultaneously as if out of nowhere, which seemed very genuine and actually worked, but all of which had similar malicious content hidden inside. The temporal connection and the uniform nature of the malicious content suggest that a single party is behind the publication of all of these, and the scope of the operation and the quality of the scam applications in turn indicate an advanced, probably state-owned actor. In many cases, the target was efficiency products used in workplaces, such as PDF editing tools and text compression applications. Some harmful content was also found in leisure apps, such as recipe and cooking apps. However, the common denominator in all of them was the novelty of the application, the use of artificial intelligence in action, the unknown nature of its publisher and the apparent functionality of the application. The applications appeared to be outwardly competent and well-coded, and they also often passed a superficial security check or managed to sneak through firewalls or scanners. They were observed around the world and in several different languages, but most cases were observed in Europe and North America. The current study focused especially on applications intended for computers, but similar harmful content can also be found in an ever-increasing amount in mobile device app stores.

In practice, there is nothing new in the dissemination of malicious content through seemingly functional applications or specifically in the pursuit of an impact on work devices. What makes the case noteworthy is that criminals have been able to take advantage of the boom in the use of AI applications. Many organisations are trying to make their operations more efficient with the help of artificial intelligence and therefore allow employees to openly try out different applications. This is exactly what criminals are trying to exploit. Normally, new applications or applications from unknown sources would be approached with quite a bit of suspicion, but in the case of AI applications, the threshold seems to be lower. In addition, when applications are being created at a high pace anyway, the wave of harmful content does not stand out so easily from the masses. In the past, the main method of criminals has been to imitate trusted applications, such as Microsoft's Office products, but now there is no similar need, as even new applications from completely unknown manufacturers easily end up in test use.

In addition, the use of artificial intelligence has made operations more efficient in the creation of applications. Many of the malicious applications detected by Trend Micro made significant use of AI-generated code, and AI had also been used to hide malicious content or trick scanners. In other words, artificial intelligence has made it easier to create malicious content in itself and perhaps at the same time freed up criminals' resources for other activities. Even now, in many cases, various digital certificates had been obtained for AI applications containing malicious content, which affected how easily they were identified as malicious content. Part of the reason for this may be that it is easier and faster to create the content itself, which leaves more time to confirm reliability.

Although the actual perpetrator of the wave now detected remained in the dark, this activity is widely carried out by both financially motivated criminals and state actors. The AI boom benefits cybercriminals in many different ways, and although the technology definitely also has clear benefits in cyber security and in improving the efficiency of work in general, it is always worth paying very close attention to the purpose for which artificial intelligence or applications that utilise it are acquired. It is also important to make sure of the manufacturer and its reliability, and a quick Google search or even asking an AI search engine may not be enough for this.

3 FOLLOW THESE

3.1 The EU vs. Privacy

In September, the EU continued its work to improve the security of the internet, or alternatively, aggressively pushed forward surveillance systems that violate the protection of privacy and the basic structures of it. Several EU legislative initiatives progressed and were in the headlines, as both supporters and opponents were quick to express their opinions. In particular, the Chat Control regulation was on the agenda, in which legislators aim for the possibility of monitoring and monitoring end-to-end secure messaging applications, such as Whatsapp and Signal. The aim is to increase the opportunities to intervene in harmful content in these communication channels, and the regulation is justified especially by restricting the dissemination of sexual material concerning children. However, what makes the regulation problematic is that, in practice, it is technically impossible to implement surveillance without significantly weakening the security of applications or violating users' privacy. There simply exists no technical solution, and creating one would require compromising the very strong protection created by end-to-end encryption. The regulation was originally created in 2022, and although it has already been stopped or rejected several times, it seems to keep coming up again.

In September, the Member States were forced to formally adopt their position on the regulation, and a vote on it is likely to take place in October, on 14 October at the earliest. At the turn of the month, it is still difficult to estimate how the vote will turn out. On the other hand, the regulation is already publicly supported by more than ten member states, but there are also opponents. Among these is Germany, whose public opposition is believed to have an impact on several countries that are still on the fence. Even though the vote would be in favour of the decree, it does not yet mean a final decision, as there are still several steps left from the negotiating table to the statute book. However, the public vote and the position of the EU majority are very significant indicators of how the EU and with it many smaller actors react (or will react) to the conflict between official surveillance and the protection of privacy in the cyber world. The choices the EU makes between fundamental rights and monitoring systems also have a direct impact on, for example, service providers and those cooperating with the EU, who will inevitably have to adapt their own practices and solutions to comply with EU laws and regulations. Instead of a single decree being passed, this is a much more significant issue.

It is somewhat difficult to understand how Chat Control or other regulations that are being worked on - such as the regulation on the collection and disclosure of metadata to the authorities, which ended its consultation round in September - get so much support in the EU. The regulations are not only technically very challenging to implement, but also in many respects in conflict with the privacy regulations and even the EU Constitution. Moreover, many of them, like both examples, have already been rejected in the EU legislative process. A lack of understanding of politicians as well as indifference may have an effect in the background, but it is difficult to see who would ultimately benefit from their passage. Opportunities for additional surveillance would certainly be useful for the authorities, but so far, the EU has globally distinguished itself from authoritarian states exercising mass surveillance precisely by its position on respecting the privacy of citizens, for example by restricting the processing of data concerning them outside its borders. In addition, the backdoor to messaging applications required by the Chat Control Regulation, for example, would also constitute a theoretical means for more than just the authorities to monitor communications, and for example, foreign APT groups and financially motivated cybercriminals would certainly be interested in trying out whether the backdoor could be expanded discreetly.

It is difficult to see who is actually benefiting from the EU's privacy-violating regulations. Invariably, the ongoing legislative processes arouse significant opposition from both citizens and information security experts. Even though it now seems that under pressure, decision-makers may eventually take a stand against Chat Control, it is only a matter of time before it is brought up again. How tough is the resistance then?

3.2 Is AI the future of politics?

Last month Albania made history by appointing the world's first AI minister, Diella. "She" is supposed to be responsible for anti-corruption work as the minister for public procurement. The idea is that AI will be incorruptible, and thus all public funds spent on public projects will indeed be spent on those projects. Diella has been heavily humanised: she even has an avatar and a voice that have been commissioned from one of the country's actresses. Dressed in traditional Albanian clothing, she is supposed to promote trust in the government. Before becoming a minister, Diella was working as an AI-powered virtual assistant, guiding applicants through the process to obtain official documents on the Albanian e-Albania platform.

In addition to stopping corruption, Diella is also supposed to make public biddings faster, more efficient and totally accountable. While the first two – speed and efficiency – are easy enough for an AI tool to achieve, accountability and the fight against corruption are not as clearcut. First of all, what accountability does an AI model have? That is a question that has been asked recently after a 16-year-old boy committed suicide. According to his parents, it was ChatGPT that encouraged him and thus they sued OpenAI, accusing it of causing the death. The lawsuit is likely to become a basis for future cases globally, but until then it is hard to say whether an AI minister will actually have any accountability at all.

One could easily think that a machine is incorruptible and only bases its decisions on cold hard facts, but that is not necessarily the case with AI. All AI models are trained on some sort of data, and in this case, it seems the data at least partially consisted of previous Albanian decisions, i.e. the "incorruptible" minister will base its future decisions on examples of corrupt ones. This is a problem with AI in general: if the data a model learns from is somehow flawed, the model itself will be too. It opens up a possibility for hostile actors to purposefully corrupt the model by injecting their own material into the data it learns from. Russia, for example, is doing this by creating huge amounts of fake news sites that only exist to skew the narrative in their favour when it comes to AI models that learn from data on the internet.

That said, if the data the model learns from is appropriate, this could actually be a very good way to ensure less corrupt government processes. The Prime Minister of Albania, Edi Rama, even goes on to say that the most important reason to have Diella is to put "pressure on other members of the cabinet and national agencies to run and think differently." In other words, this is a threat: if other ministers do not give up their corrupt ways, their jobs can be taken by AI as well. If such a wide proliferation of AI at the highest levels of politics was to happen, the effects of data corruption could be catastrophic. In that case, it is crucial to look for new ways to ensure the data that is used to train important AI models is as appropriate as possible, with no way for adversaries to tamper it.

Other nations will undoubtedly be following the implementation and results of the new minister of public procurement. If all goes well, perhaps we will soon see similar experiments in other countries too. For now, it is best to approach the subject with a healthy dose of scepticism but also remember that it is no longer just a part of science fiction. AI is here to stay, and it will permeate every layer of society, including the very top.

REFERENCES:

Events in the cyberlandscape

Cyberwatchin weekly reviews September 2025

https://www.bbc.com/news/articles/cx2rdlj8ejgo

https://yle.fi/a/74-20185555

https://understandingwar.org/research/russia-ukraine/warning-russia-may-be-planning-violent-protests-after-the-moldovan-elections/

https://www.hs.fi/maailma/art-2000011493540.html

https://www.ransomware.live/group/datacarry

The current state of spyware

https://security.apple.com/blog/memory-integrity-enforcement/

https://www.techradar.com/computing/cyber-security/apple-may-have-found-a-fix-for-mercenary-spyware-attacks-and-iphone-17-and-iphone-air-users-will-get-the-most-of-new-protections

https://thehackernews.com/2025/09/apple-iphone-air-and-iphone-17-feature.html

https://therecord.media/us-investors-in-spyware-tripled-in-2024

https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/mythical-beasts-diving-into-the-depths-of-the-global-spyware-market/

The diverse threats to aviation in Europe

https://www.securityweek.com/european-airport-cyberattack-linked-to-obscure-ransomware-suspect-arrested/

https://www.euronews.com/next/2025/09/21/what-do-we-know-about-the-cyberattacks-that-hit-europes-airports

https://www.bbc.com/news/articles/c62ldxyj431o

https://areena.yle.fi/1-72480902

The AI boom offers opportunities for criminals

https://www.trendmicro.com/en_us/research/25/i/evilai.html

https://www.tomsguide.com/computing/malware-adware/more-than-250-malicious-apps-are-spreading-info-stealing-malware-on-android-and-ios-delete-these-right-now

The EU vs. Privacy

https://www.theregister.com/2025/09/11/eu_chat_control/

https://chatcontrol.fi/

https://edri.org/our-work/chat-control-what-is-actually-going-on/

Is AI the future of politics?

https://www.bbc.com/news/articles/cm2znzgwj3xo

https://www.politico.eu/article/albania-apppoints-worlds-first-virtual-minister-edi-rama-diella/

https://www.bbc.com/news/articles/cgerwp7rdlvo

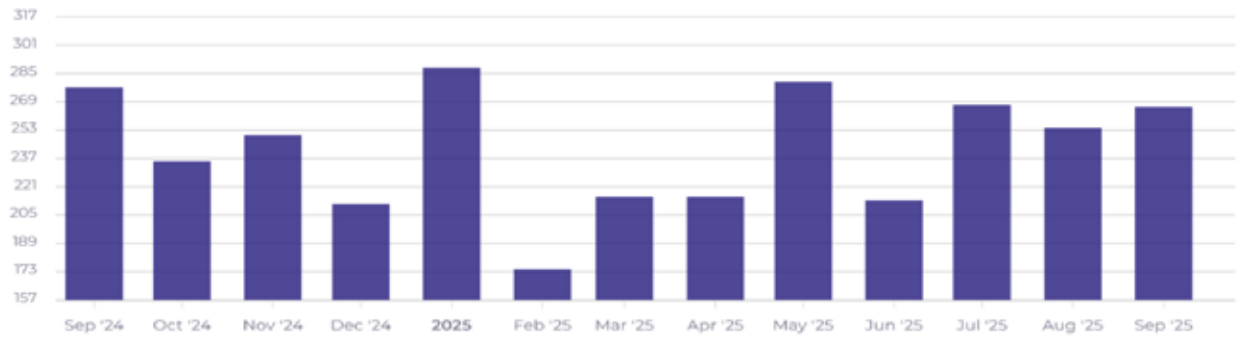
Cyberwatch MONTHLY REVIEW

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

THREAT INTELLIGENCE REVIEW

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

Major cyberattacks and campaigns



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

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

ASAHI-BREWERY'S CYBERATTACK IN JAPAN

DATE: 29.9. onwards
DESCRIPTION: The production facilities of Japan's most popular beer brand, Asahi, were targeted by a cyberattack involving ransomware in the last week of September. The cyberattack has brought the majority of the company's production facilities to a standstill. At the moment, the company is unable to accept new orders, and production has not been restarted at all facilities.
THREAT ACTOR: So far, no hacker group has claimed responsibility for the cyberattack. Asahi has also not disclosed who is behind the attack.
MOTIVE: Preliminary information points to a financial motive that often underlies these types of cyberattacks.
IMPACT: The attack underlines the impact of cyber threats in the brewery or, more broadly, in the food industry. As a result of the cyberattack, the company's production operations have mainly been suspended, and the products it produces are expected to run out of stores within a week.

SECRET NETWORK OF SIM SERVERS AT THE UN MEETING PLACE

DATE: Early September 2025
DESCRIPTION: The U.S. Secret Service seized more than 300 SIM servers in the New York City area ahead of the start of the UN General Assembly. The network had previously been used to send anonymous assassination threats to several US officials.
THREAT ACTOR: Unknown, but has connections to as yet undisclosed state actors
MOTIVE: Unknown, but connections to state actors suggest a political motive
IMPACT: In addition to sending anonymous threats, the network would have made it possible to cripple the entire New York phone network, carry out denial-of-service attacks, and conduct encrypted conversations between threat actors and criminals. Although the effects were now minor and limited to the United States, it is hardly a coincidence that the network was set up at the venue of the UN General Assembly. However, at least until the investigation proceeds, it is impossible to say who actually had plans for the use of the network and what those plans were.

IRAQI PERSONAL DATA SYSTEM BREACH

DATE: 22.09.2025
DESCRIPTION: A hacker group called Cyberdragons (Cyb3rDrag0nz) hacked into Iraq's personal data system in September and managed to steal about 32 gigabytes of data. There is a wide variety of data, but it has been speculated that it contains a significant amount of sensitive information from Iraqi citizens.
THREAT ACTOR: Cyberdragons
MOTIVE: Most likely political
IMPACT: Cyberdragons shared the database they stole on their open Telegram channel, which is likely to lead to scams and identity theft targeting Iraqis. There is no full knowledge of why and how Cyberdragons choose their targets, or the motivation for attacks. The group operates almost exclusively in the Middle East but has attacked both Islamist targets and those who support Israel. However, it is not known to have carried out extortion strikes or otherwise pursued direct financial gain.

DATAMILJÖ BREACH

DATE: Attack took place at the end of August, information leaked 9.9.2025
DESCRIPTION: A Swedish company that provides IT services to local municipalities and other entities was the victim of a data breach at the end of August. Behind the attack is a relatively unknown ransomware actor called Datacarry, which ended up uploading the stolen database to the dark web in September. The reason for this is likely either failed negotiations or refusal to pay ransom.
THREAT ACTOR: Datacarry
MOTIVE: Financial
IMPACTS: The personal data of more than one million Swedes ended up on the dark web. The disclosure of the information is likely to lead to identity theft, follow-up scams, and phishing.

Active and rising threat actors

SCATTERED SPIDER

DESCRIPTION: Scattered Spider is a cybercriminal group that consists of teenagers and young adults believed to be mainly from the United States and the United Kingdom. It has had a wide range of victims including hotels and banks.
RECENT ACTIVITY: Along with several other ransomware and cybercrime groups, the group announced its ”retirement” in September on the popular BreachForums discussion forum and its Telegram channels. However, just a few days later, there were reports of new attacks by the group on financial sector organisations.
METHODS AND TACTICS: The group uses social engineering, such as phishing emails, SIM swapping, and attacks that exploit weaknesses in multi-factor authentication. Often, the end result is to install ransomware on the victim's systems and blackmail them with data.

TURLA AND GAMAREDON

DESCRIPTION: Turla and Gamaredon, threat actors linked to Russia's FSB security service, have been active for more than a decade. Their tasks include engaging in cyber espionage and carrying out state-sponsored cyberattacks on targets around the world.
RECENT ACTIVITIES: In the past, Russian security services and their internal departments have been observed competing with each other and even undermining each other's work. This perception is undergoing a transformation. Cooperation between Turla and Gamaredon has been observed in cyberattacks targeting Ukraine. The phenomenon must be monitored, but closer cooperation may mean more serious Russian cyberattacks in the future.
METHODS AND TACTICS: Gamaredon is known for precise spear phishing to gain access to the victim's systems. Turla, on the other hand, has become known for the Trojan malware that bears its name, but it has also developed several other customised malware.

AKIRA

DESCRIPTION: First detected in March 2023, Akira is a threat actor with strong links to a Russian Conti-ransomware hacker gang that went out of business around the same time. Akira operates on the principle of the RaaS operating model, offering the malware developed by it to subcontractors for a fee.
RECENT ACTIVITY: In Finland, Akira is especially known for the series of attacks on Finnish organisations at the end of 2024. The group's activity has fluctuated over the past year, but it rose to the top of the statistics again in September in terms of new victims.
METHODS AND TACTICS: Employs malware of their own development, which is thought to be based on Conti's tools. Once it has broken into the target, it encrypts and steals information, after which a notification of the operation is published on dark web sites. In addition, attacks and ransom demands carried out by Akira's subcontractors are also published. The ransoms range from hundreds of thousands of dollars to a few million, depending on the size of the target organisation.

Services

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

Cybersecurity Capacity Building

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

1. STARTING POINT

- Cyber matuCheckingrity
- Web analysis and attack surface analysis
- Operational environment analysis

2. ESTABLISHING OPERATIONS

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

3. TRAINING FOR MANAGEMENT AND STAFF

- Producing information about cybersecurity through training while operations are ongoing
- Operational environment analysis: weekly and monthly review
- Scenario training with the customer

4. MONITORING

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

5. SUPPORTING DEVELOPMENT

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

6. CONTINUITY MANAGEMENT

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

Operational Environment Analysis

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

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

More information: info@cyberwatchfinland.fi

WEEKLY REVIEW

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

CYBERWATCH MAGAZINE

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

MONTHLY REVIEW

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

SPECIAL REPORTS

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

Web Analysis - darkSOC®

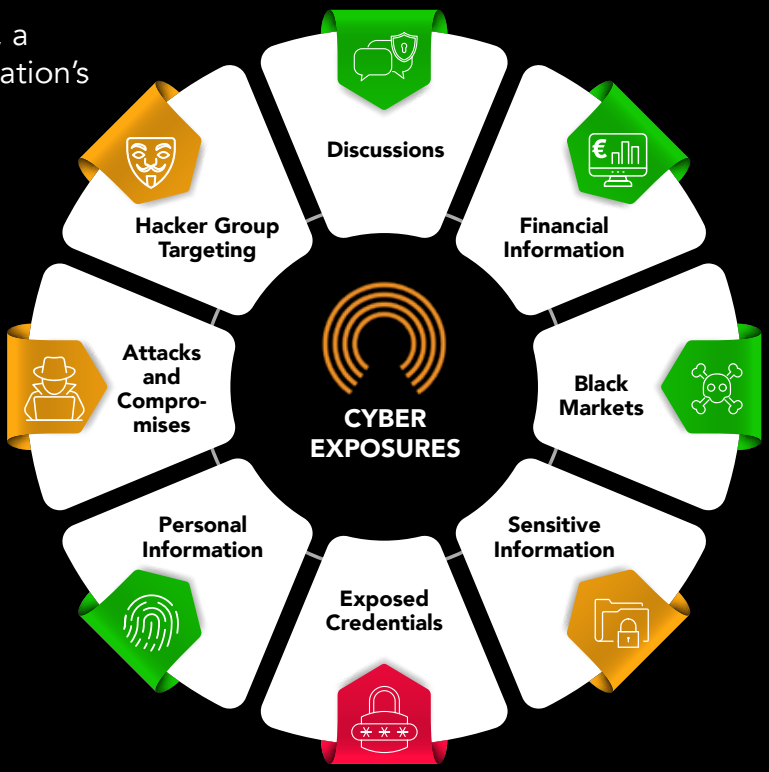
WEB ANALYSIS

DarkSOC® dark and deep web analysis

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

Attack surface analysis

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



MONITORING

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

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

Security of the Supply Chain

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

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

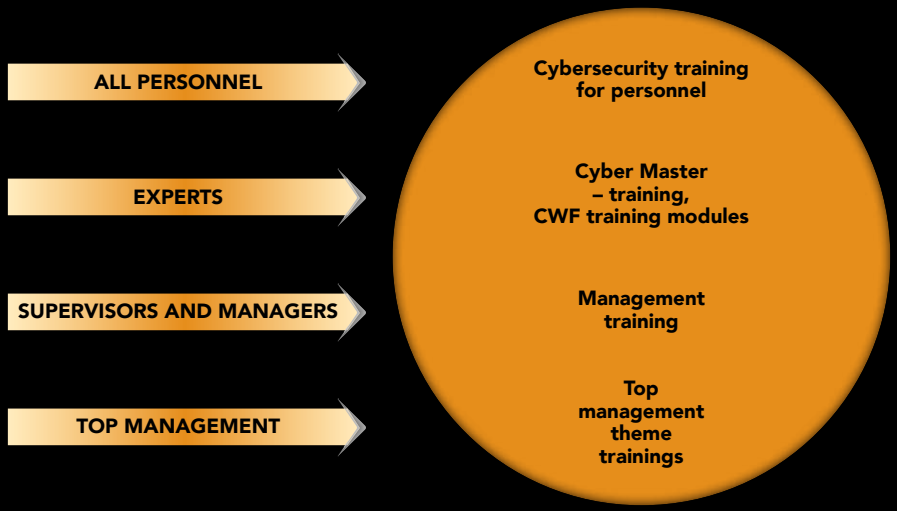
The analysis can be done for selected parts of the supply chain organisations (requires an agreement). The findings of the attack surface analysis are introduced to the concerned organisations which are responsible for the implementation of corrective actions and reporting to the customer when the corrective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

An example of service content:

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

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

Training and Competency Development



CYBERWATCH TRAINING MODULES AND LECTURES

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

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

Examples of training modules:

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

Examples of lectures:

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

CYBER SITUATIONAL AWARENESS FOR PERSONNEL

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

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

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

MIF TRAINING PROGRAMS

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

Cyber Master Basics

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

Content of the Training:

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

Cyber Master Extended

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

Content of the Training:

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

CURRENT COURSE CONTENT

OUR COURSES' CONTENT, ALSO AVAILABLE ON CYBER MASTER BASIC

Training day 1

Theme:
Operating environment and management

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

+ Assignments

Training day 2

Theme:
Cyber risk management

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

+ Assignments

Training day 3

Theme:
Cyber resilience

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

+ Assignments

TRAINING DAY COVERS FOLLOWING ISO27001 REQUIREMENTS:

Training day 1:
4 Context of the organisation
5 Leadership

Training day 2:
6 Planning

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

OUR COURSES' CONTENT, ALSO AVAILABLE ON CYBER MASTER EXTENDED

Training day 1

Teema:
Cybersecurity preparedness

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

+ Development project +assignments

Training day 2

Teema:
Kyberturvallisuuden vaste

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

+ Assignments

TRAINING DAY COVERS FOLLOWING NIST FUNCTIONS:

Training day 1:
Govern, Identify, Protect

Training day 2:
Detect, Respond, Recover

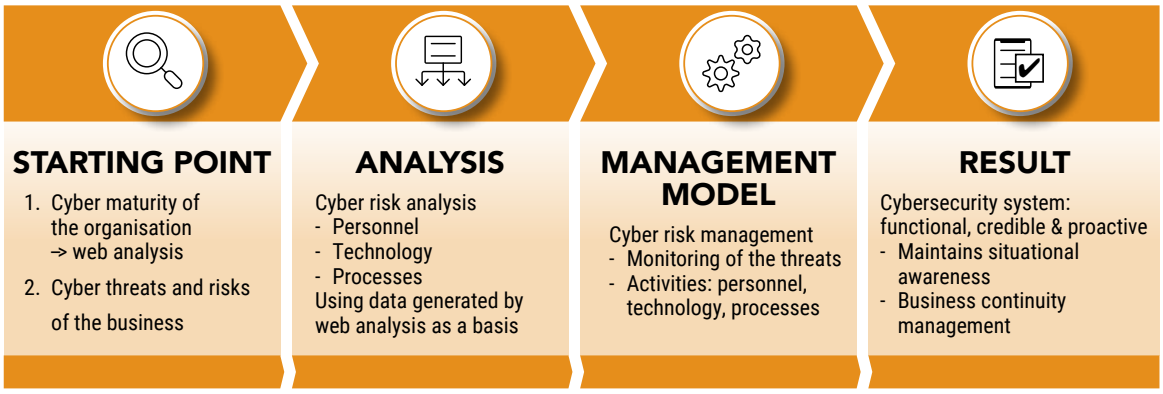
Cyber Risk Management Model

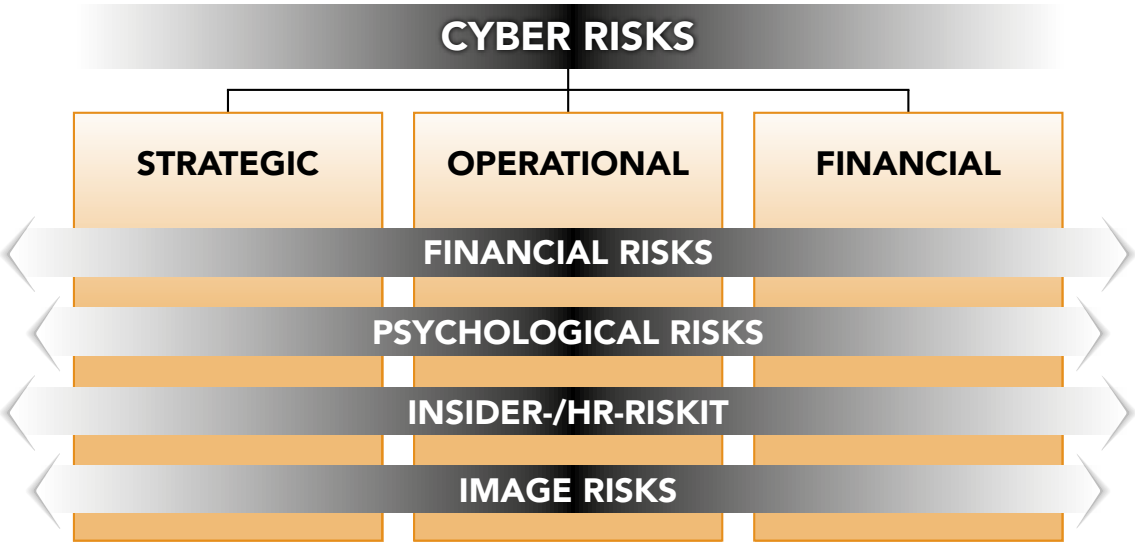
Cybersecurity needs to be increasingly considered in different stages of the business plan. A comprehensive cybersecurity risk management plan will provide a roadmap for how to better address cybersecurity threats and implement the required actions brought by the increasing EU regulation and national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

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

The cyber risk management model process consists of four stages:

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





NIS2 Consulting Service

Cyber Security Directive (NIS2)

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

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

Entities are divided into critical sectors and other critical sectors.

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

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

WE SUPPORT COMPANIES IN IMPLEMENTING THE NEW LEGISLATION.

We provide assistance with:

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

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

Management Advisory Services

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

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

Cyber Due Diligence

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

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

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

FOR A BETTER DIGITAL FUTURE

MESSUKESKUS
The real social media

Join the leading minds in cyber security at Cyber Security Nordic 2025. Experience world-class talks, fresh insights, and inspiring keynotes on the most pressing issues in the field.

Among the keynote speakers are:

Philip Stupak Senior Director for Advocacy, ISC2

Philip Stupak, former Assistant National Cyber Director at the White House, has shaped U.S. cybersecurity policy at the highest level. At ISC2, he represents the global cybersecurity profession to policymakers worldwide, building on his leadership in advancing President Biden's cybersecurity strategy.

Andžejus Roginskis Head of Digital Support Unit, Europol EC3

Andžejus Roginskis leads Europol's Digital Support Unit at EC3, supporting complex cybercrime investigations across the EU. With over 30 years in law enforcement, he brings deep expertise in cyber intelligence, digital forensics, and cryptocurrency tracing.

CYBER SECURITY NORDIC

4–5 November 2025
Helsinki Expo and Convention Centre

cybersecuritynordic.com