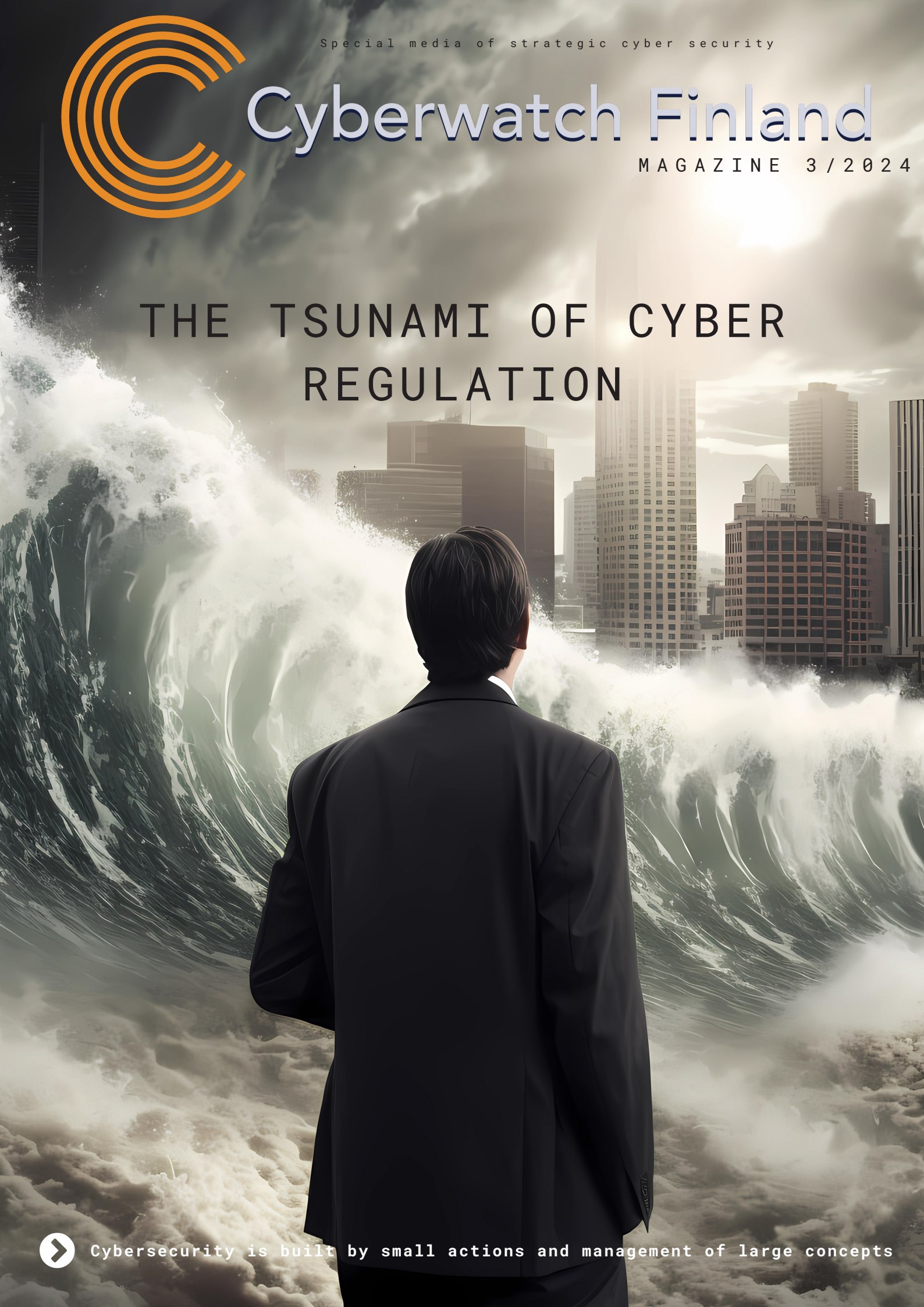
Special media of strategic cyber security

Cyberwatch Finland

MAGAZINE 3/2024

# THE TSUNAMI OF CYBER REGULATION



Cybersecurity is built by small actions and management of large concepts

# CONTENT

3/2024

**Cyberwatch Magazine**

Special media of strategic cyber security

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

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

Subeditor
Elina Tuomisto
elina@cyberwatchfinland.fi

LAYOUT
Elina Tuomisto
elina@cyberwatchfinland.fi

ILLUSTRATIONS
Gencraft
Pixabay
Shutterstock

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

PRINT HOUSE
Scanseri Oy, Finland

Editorial

# REGULATION TSUNAMI IS COMING, ARE WE READY

// Aapo Cederberg

The current geopolitical environment is highly unstable, particularly due to Russia's war of aggression against Ukraine. Russia sees itself as waging a kinetic (traditional) war in Ukraine and a hybrid war against Western civilization. This has changed our security environment forever. Critical infrastructure has been the main target of kinetic and non-kinetic attacks. Cyber warfare in Ukraine has had less impact than expected. Russia seems to prefer to use conventional military force in Ukraine, which has greater destruction and deterrence, than smart cyber operations, which, once exposed, will be difficult to reuse.

It seems that the smartest cyber operations will be saved as hybrid influencing tools against Western countries. This allows operating below the threshold of conventional war and creates information-psychological deterrent effects. Cognitive warfare has become a strong part of asymmetric warfare. The aim is to undermine citizens' mental crisis resilience through long-term hybrid operations. There is no end in sight to the war, so we must invest more and more in securing society's critical functions and services. Contingency measures must cover the whole of society and all actors.

The EU Cybersecurity Directive NIS2, which entered into force at the turn of the year, will be implemented through a new national cybersecurity act. The aim is set for the act to enter into force in October 2024. The act sets out how to put into practice the obligations of the directive with regard to private companies. In the public sector, the obligations are laid down by updating the Information Management Act. The changes are significant. Critical entities will have to update their cybersecurity arrangements, taking into account the requirements of the NIS2 Directive and national legislation. The new obligations cover cybersecurity risk management, management responsibility, incident reporting and registration on the list of operators maintained by the competent authority by the end of 2024. Cybersecurity will thus become mandatory, especially for key actors, and failure to comply with obligations may lead to fines.

In my opinion, this process should be viewed as a positive development, the cyber threat continues to grow and we all need to take development measures anyway. The new legal obligations focus on the right things that need to be in order for us to better respond to the future challenges of the cyber world.

The ECI Directive on European Critical Infrastructure Protection will be replaced by new CER-directive (Critical Entitied Resilience), also known as the resilience directive. CER is based on the EUs Security Strategy, which stated, among other things, that "critical infrastructure used in our daily lives must be secure and sustainable". The scope of the directive covers eleven sectors: transport, energy, banking, financial, health, water and sanitation, food, digital infrastructure, public administration and space sectors. This must go hand in hand with the cybersecurity directive, especially since critical infrastructure is the main target of cyberattacks. In the financial sector, risk management must comply with the DORA regulation, which is much more detailed than the NIS2 regulation.

All this regulation aims to harmonise and improve the level of cybersecurity across the EU. This is particularly important from the perspective of strengthening competitiveness and digital autonomy. Corporate boards and operative management must understand that we are not only preparing for threats and risks, but also monitoring our own competitiveness and creating new business opportunities. According to the NIS2 regulation, the executive management is responsible for organising cybersecurity risk management and supervising its implementation. The cybersecurity risk management operating model must be approved by the executive management, and the management must also have an up-to-date picture of the state of the company's cybersecurity.

In August, we published a white paper on the challenges and resilience of the modern digital society. Our goal is to stimulate discussion about the state of cybersecurity and share our conclusions from the war in Ukraine. In Finland, the role of the private sector in proposing initiatives could be stronger and think tank activities could be increased. We believe that the white paper itself is a suitable format for presenting new ideas. Our intention is not to criticise anyone, but to think out loud. The feedback we have received has been very positive and encouraging. The white paper is freely available on our website. Hopefully the debate will continue.■

**AAPO CEDERBERG**

- Managing Director and Founder
- **Cyberwatch Finland**

# ON THE CREST OF A WAVE OF CYBERSECURITY REGULATION

// Jukka Lång, Joona Linner and Johanna Tuohino

New regulation around cybersecurity is building up in a rapid and EU-driven way. In the autumn of 2024, we are on the crest of a tidal wave on the way to applying the inevitably progressive new cybersecurity regulation. This regulatory framework includes legislation aimed at creating an EU-wide framework for cybersecurity management and improving the security of products, critical infrastructure and actors in the EU's internal market, among others.

The NIS2 ((EU) 2022/2555) and CER ((EU) 2022/2557) Directives are particularly topical this autumn and are addressed below. Before doing so, let's take a brief look back at existing cybersecurity regulation.

## THE EU GENERAL DATA PROTECTION REGULATION OBLIGES THE SECURITY OF PROCESSING OF PERSONAL DATA

One of the most important elements of existing cybersecurity regulation is contained in the EU General Data Protection Regulation (EU) 2016/679 (the "GDPR"). The elements of the GDPR provide a cybersecurity baseline for the processing of personal data that is applicable to all businesses and other organisations in the EU's internal market. The GDPR also imposes data security obligations on organisations that are not subject to sector-specific cybersecurity regulation. Data security (integrity and confidentiality) is one of the data protection principles under the GDPR, i.e. one of the core principles applicable to processing of personal data. Other cybersecurity-related elements of the GDPR include provisions on data protection impact assessment (DPIA) and data breach reporting and notification to data subjects. The obligation to enter into a data processing agreement between the controller and the processor of personal data in accordance with the GDPR, as well as the related provisions of international data transfers, is part of ensuring the security of supply chains.

These above-mentioned elements are important alongside the new cybersecurity regulation, as data protection and cybersecurity regulation and their requirements often lead to overlapping or parallel requirements in areas such as incident management and ensuring security of supply chains. In some cases, data protection and data security must also be considered in parallel.

## THE EU CYBERSECURITY ACT AS A BASIS FOR SECOND-GENERATION CYBERSECURITY REGULATION

The so-called first-generation of European cybersecurity regulation refers to the Network and Information Security (NIS) Directive (2016/1148) and the European Critical Infrastructure (ECI) Directive (2008/114EC). The NIS2 Directive, which replaces the NIS Directive, is broader in scope than its predecessor. The CER Directive, discussed below, replaces the ECI Directive.

The EU Cybersecurity Act ((EU) 2019/881) is the basis for the second-generation of cybersecurity regulation. The Cybersecurity Act established the European Union Agency for Cybersecurity (ENISA) and the framework for European cybersecurity certification. The future objective of EU legislators is that the relevant standards under the certification framework of the Cybersecurity Act will be applied by the entities covered by the NIS2. For the time being, the implementation of the certification schemes at the EU level is still pending. Currently, the certification standards have been established for smart cards, microchips and digital wallets.

## NIS2 DIRECTIVE EXTENDS CYBERSECURITY RISK MANAGEMENT OBLIGATIONS IN CRITICAL SECTORS

On 23 May 2024, Finland took a significant step towards strengthening its cybersecurity legislation when the Government submitted a proposal (HE 57/2024 vp) to Parliament to implement the NIS2 Directive with the Cybersecurity Act and amendments to the Information Management in Public Administration Act. The aim of this regulation is to enhance cybersecurity in critical sectors and to shift the regulatory focus to cybersecurity risk management and incident reporting. The regulation is aimed to be applicable from 18 October 2024.

## BASIS OF THE NIS2

The NIS2 Directive and its national implementation broaden the scope of cybersecurity requirements significantly, covering medium and large entities in critical sectors. These sectors include energy, transport, healthcare, digital infrastructure, as well as entirely new sectors such as public administration, food production, waste management and certain industries not covered by the predecessor (NIS Directive). It is noteworthy that the new requirements apply to certain entities regardless of size, such as providers of public electronic communications networks and services. In addition, certain covered entities are in the category of essential entities and therefore subject to stricter supervision and more severe sanctions.

For entities in critical sectors identified in the NIS2, the regulation applies to the entity as a whole (to the legal person). According to the general rule, the country where an entity (legal person) in a sector under the scope of NIS2 is established determines which Member State's national regulation is applicable. For the ICT service management and digital infrastructure sectors, the territorial applicability of the NIS2 is exceptionally determined by the place of establishment of the entity at European level.

Entities subject to NIS2 will need to reassess and update their cybersecurity practices in relation to the new cybersecurity requirements. The new requirements will cover cybersecurity risk management, management accountability, incident reporting and registration in the registry of entities maintained by the competent authority by the end of 2024.

The new requirements are also likely to change contracts and contractual terms related to cybersecurity of ICT systems beyond the sectors covered by the NIS2.

## CYBERSECURITY RISK MANAGEMENT

Entities must adopt a comprehensive cybersecurity risk management approach. The policy shall include technical, operational and organisational measures designed to protect the entity's communication networks and information systems and mitigate the adverse effects of incidents. The key elements of the risk management model are:

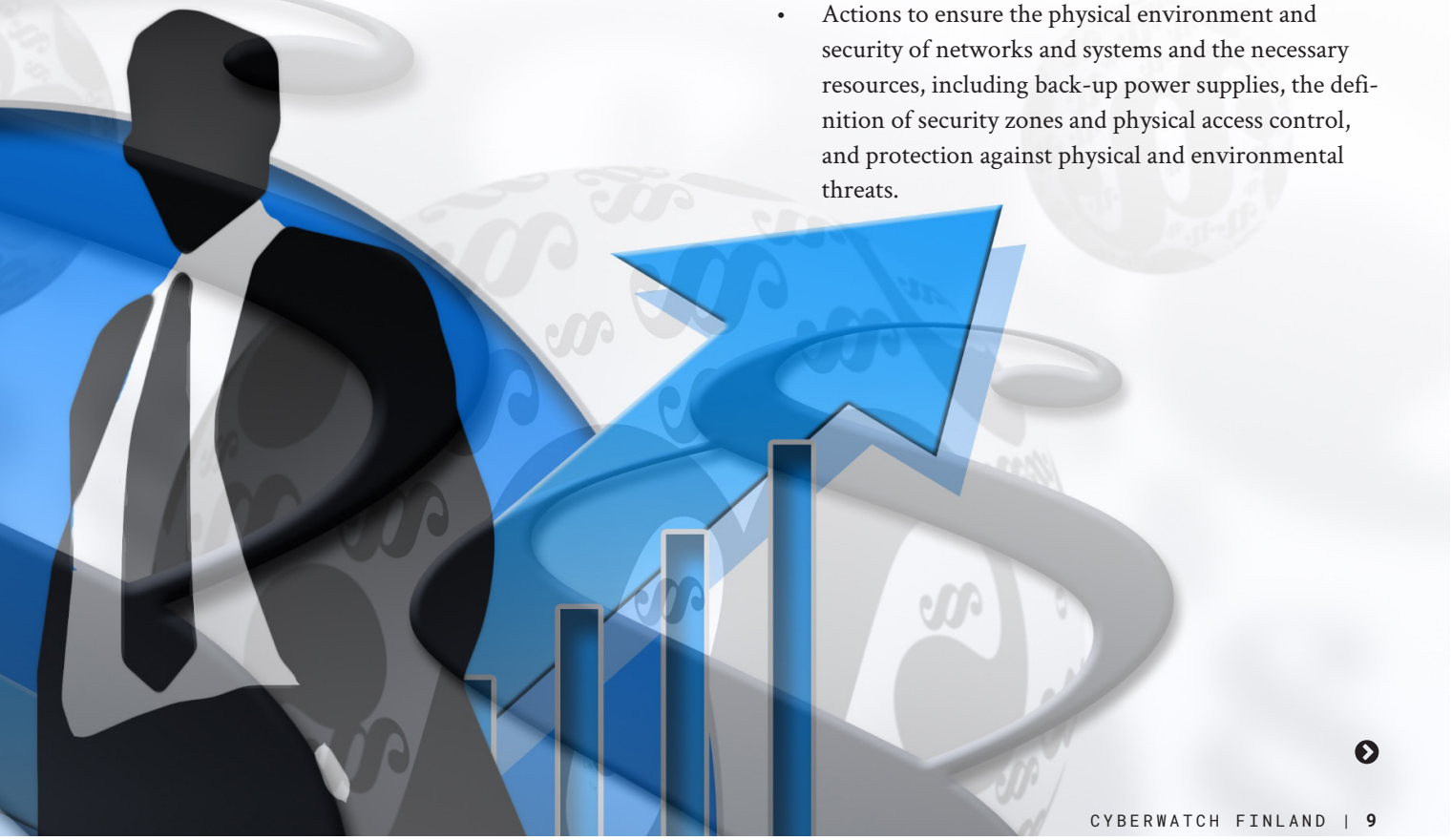
- **Risk assessments and analyses:** The model must be based on risks and all-hazards approach, so that entities can proactively identify and address potential threats from different sources.
- **Documentation:** Entities must define, describe and document their risk management objectives, processes and responsibilities. The documented risk management policy must be kept up to date. The policy shall be approved by the top management of the entity.
- **Minimum risk management measures:** The risk management model must include at least the minimum measures listed in the legislation.

## MINIMUM OBLIGATIONS FOR THE CYBER RISK MANAGEMENT MEASURES

The cybersecurity risk management approach must take into account the minimum obligations required by the NIS2. The following themes should at least be considered when assessing and implementing the necessary management measures:

- Network and system security policies and risk management policies;
- Policies and processes for evaluating the effectiveness of management measures defined under the model;
- Security in the acquisition, development and maintenance of networks and systems, and the identification and handling of vulnerabilities:
    - (i) Determination of criteria for supplier selection and associated risk assessments, (ii) the secure development lifecycle, (iii) configuration and change management, (iv) patching and maintenance, (v) security testing, (vi) update management, (vii) network security and segmentation, (viii) protection against harmful and unauthorized software, and (ix) vulnerability handling and disclosure;

- Supply chain security, including security policies, contracting practices and lists of suppliers and service providers;
- Asset management, including asset classification and handling, policies on terminal equipment and storage devices, asset lists (inventory), and the restoration and destruction of assets, including as part of human resources security;
- Human resources security (including suppliers' personnel), such as background checks, contractual terms and disciplinary procedures, and procedures for dismissal and change of duties;
- Access management and authentication procedures, including access management policies and, where applicable, multi-factor authentication (MFA) and possible continuous authentication solutions;
- Policies and procedures for the use of encryption and cryptography, including associated risk assessments, data classifications and the levels of encryption to be applied to different categories;
- Detection and handling of incidents to recover and maintain security and reliability:
    - (i) incident management policy, (ii) monitoring and logs, and other activities from which hazard indicators can be collected, (iii) incident assessment and classification, (iv) incident response, and (v) root cause assessment and other follow-up actions to reduce the risk of a similar incident occurring in the future;
- Back-ups, business continuity and crisis management, including associated plans and, if necessary, the deployment of backup communication systems;
- Basic level security practices and awareness, including security exercises and basic cyber hygiene practices, basic awareness raising and additional training/ exercises based on task-specific risk assessments (tailored in-depth training);
- Actions to ensure the physical environment and security of networks and systems and the necessary resources, including back-up power supplies, the definition of security zones and physical access control, and protection against physical and environmental threats.



## MANAGEMENT RESPONSIBILITY

Under the proposed NIS2 legislation, the entity's management is responsible for organising cybersecurity risk management and overseeing its implementation. The cybersecurity risk management policy must be approved by the entity's management, which must also have an up-to-date view to the entity's cybersecurity status.

In Finland, the management of an entity is defined as the members of the board of directors and the supervisory board (and their deputy members, where applicable) and the CEO. In addition, the management of the entity may also mean other persons who effectively manage the activities of the entity.

The defined management responsibility highlights the need and requirement for management to have sufficient understanding of cybersecurity risk management and the need to review internal decision-making and reporting processes in order to effectively take responsibility for cybersecurity management in accordance with NIS2.

## SUPPLY CHAIN SECURITY

New cybersecurity risk management requirements mean that supply chains in particular need to be reassessed. Entities need to consider the overall quality of products and services, integrated risk management and cybersecurity practices of their direct suppliers. It is the responsibility of the entities to ensure that the selected and used products and services meet the cybersecurity requirements of their risk management model. In practice, this means, for example, reviewing contractual terms with suppliers.

It is worth noting that the supply chain security requirements apply to the regulated entity, but the obligations do not apply directly to the entity's system or equipment suppliers. Suppliers may themselves be under the scope, but in this case, they will look at risk management from the perspective of their own operations.

## INCIDENT REPORTING

Incident reporting is at the heart of the new cybersecurity regulation and failure to report can lead to the imposition of an administrative sanction.

Entities shall report significant incidents to the competent supervisory authority following the next reporting process:

1. First notification within 24 hours of detection of a significant incident.
2. Follow-up notification within 72 hours of detection of a significant incident.
3. Final report not later than one month after the follow-up notification or the end of the processing.

It is a **significant incident** if it causes or may cause any of the following:

- → serious **disruption** of the services;
- → a significant **financial loss** to the entity; or
- → substantial **material or non-material damage** to other natural or legal persons.

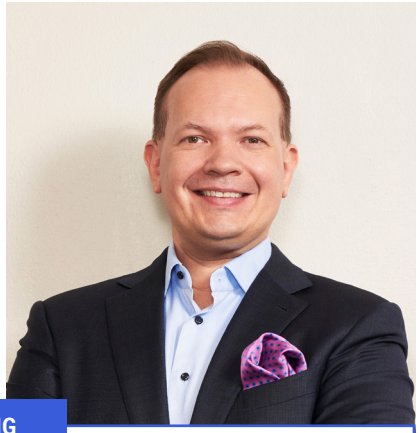
The detailed guidance and interpretation of the definition of a significant incident is expected to be clarified in the near future by the European Commission's implementing regulation and supervisory authorities' guidance.

## SUPERVISORY AUTHORITIES AND ENFORCEMENT

In Finland, supervision of the NIS2 legislation is decentralised. The sectoral supervisory authorities will monitor compliance in their respective areas of responsibility. For example, the Finnish Transport and Communications Agency (Traficom) supervises digital infrastructure entities, while the Energy Authority supervises electricity entities. An entity operating in several sectors may be subject to supervision of several supervisory authorities.

The National Cyber Security Centre at Traficom acts as a contact point and coordinates the activities of the supervisory authorities. In addition, a national CSIRT unit will be set up within Traficom, which will play a key role in monitoring, analysing and assisting with cyber threats and incidents.

The NIS2 gives supervisory authorities extensive powers, including access to information, inspection rights and the possibility to issue orders and warnings.




**JUKKA LÅNG**

- Partner, Head of Data Protection & Cyber Security, advocate, CIPP/E
- Jukka Lång is in charge of Dittmar & Indreniuksen Data Protection & Cyber Security -competence area. Jukka is known as Finland's leading data protection expert and he is one of Finland's few partner-level advocates specialising in cyber security regulation.
- **Dittmar & Indrenius**

## RELATIONSHIP BETWEEN CER, DORA AND NIS2

While the NIS2 framework protects against all threats to communications networks and information systems and the data resources they contain, the risk management obligations under the CER Directive extend to threats that may target any other function, in addition to the ICT system, that is required to provide the service defined as critical. In addition, critical entities covered by the CER Directive do not have to assess for themselves whether they are covered by the national legislation implementing the CER Directive. The entities covered by the law will be designated separately as critical entities.

Once an entity is designated as a critical entity under the CER Directive, that entity, regardless of size, is also automatically an essential entity under the NIS2. The national law implementing the CER Directive should become applicable no later than 18 October 2024, but there have been delays in the preparation of the law, according to the information available at the time of writing this article.

DORA is the EU regulation on cybersecurity risk management applicable to financial institutions ((EU) 2022/2554), which is directly applicable in all Member States. DORA is considerably more detailed than NIS2 and financial institutions will apply DORA instead of NIS2. The DORA Regulation is already in force but will apply from 17 January 2025.

## LOOKING FORWARD

NIS2, CER and DORA are significant pieces of the new regulatory framework for cybersecurity, which extends cybersecurity risk management to the legal side. This means that entities will be guided to refine and develop their cybersecurity risk management as required by the regulation. It also means that (i) in the future, more and more lawyers will be invited (or will join on their own initiative) to participate in risk management teams and (ii) risk management will be more closely monitored by the entity's management and supervisory authorities. The ultimate goal is to create more secure services and a safer society for all of us.

## A SUMMARY OF THE KEY EU CYBERSECURITY REGULATION:

- EU General Data Protection Regulation ("GDPR") (EU) 2016/679 (applicable)
- Cybersecurity Act (EU) 2019/881 (applicable)
- Network and Information Security Directive ("NIS2") (EU) 2022/2555 and its implementing national legislation (applicable from 18.10.2024)
- CER Directive (EU) 2022/2557 and its implementing national legislation (applicable from 18.10.2024)
- Digital Operational Resilience Act ("DORA") (EU) 2022/2554 (applicable from 17.1.2025). ■


**JOHANNA TUOHINO**

- Senior Associate
- Johanna Tuohino specialises in cybersecurity, data protection, electronic communications and technology regulation. Johanna is a jurist in charge of Dittmar & Indrenius' Cyber Security team
- **Dittmar & Indrenius**



**JOONA LINNER**

- Associate, advocate, CIPP/E, Certified Digital Asset Advisor (CDAA)
- Joona Linner specialises in cybersecurity, data protection, fintech and technology regulation. Joona is one of the key forces behind Dittmar & Indrenius' Cyber Security team.
- **Dittmar & Indrenius**

# THE EU REGULATORY TSUNAMI IS HERE – IS YOUR BUSINESS READY?

// Peter Sund and Risto Rajala

The European Union has the ambition to build a better digital life for Europeans. However, the goal is not an idea that "came from Europe", but a democratically defined common will of all of us. It has chosen regulation as a means of achieving this goal, because the EU is better able to do so than many others. Although companies generally do not want more regulation, the promises of digitalisation, data economy and digital markets are unmissable in terms of business and financial well-being.

During the past parliamentary term 2019–2024, the European Commission presented dozens of legislative proposals that affect our digital lives in different ways, many of which have already passed or will soon pass the legislative processes of the Council of the EU and the European Parliament. The significantly increasing regulation has given rise to much debate, including concern and criticism. You often hear about a regulatory tsunami, and the claim is not entirely misleading. The tsunami – which is not a single big wave, but a series of multiple waves – is just reaching the "shoreline" of our digitally active businesses. At the same time, it might be worth asking how many non-digital employer companies there are in Finland at all? The winners from the upheaval will be those companies that manage to ride the crest of the regulatory wave, i.e. adopt new obligations in an agile manner, i.e. quickly and cost-effectively, thus adapting their business operations to the framework conditions set by them.

From the perspective of companies engaged in digital business, the most relevant new acts are the Artificial Intelligence Regulation, the Data Regulation, the NIS2 Directive and the Cyber Resilience Act. In practice, the content of all four of these acts is known, and the most significant attention is already focused on the launch of the implementation phase. Other statutes that have been adopted or are still being prepared will also have an impact, but mostly in a sector-specific or point-by-point manner compared to the above-mentioned acts with very broad fields of application.

The EU's Artificial Intelligence Act (AI Act) is the first comprehensive regulatory framework for AI in the world. It aims to ensure that AI systems are safe and meet the requirements of European fundamental rights standards, while promoting innovation. In practice, this seemingly fancy goal means that innovations are targeted at acceptable use cases and not, for example, at those used in China to permeate and control citizens. The regulation classifies AI systems according to their level of risk and sets stricter requirements for high-risk applications, such as those used in healthcare and transport. In addition, it completely prohibits certain uses of AI, such as real-time biometric identification in public places, unless there is a serious security threat. The Artificial Intelligence Regulation entered into force in August 2024 and will be applied within various transition periods, mainly in 2026.

The EU's Data Act aims to improve the availability and use of data in Europe. It aims to ensure that data can be shared fairly and openly, promote innovation and create a competitive data market. At the heart of this is the right of the end users of data-producing ICT technology to their own data during use. The regulation applies in particular to connected devices and services and aims to facilitate the utilisation of the data produced by them. The Data Regulation entered into force in January 2024 and its application will mainly begin in September 2025.

The NIS2 Directive aims to strengthen cybersecurity in sectors and activities important to the functioning of society, such as the energy industry and healthcare. The Directive requires organisations to put in place

effective risk management measures and report cybersecurity incidents in order to increase the level of cybersecurity across the Union. In Finland, the Government has drafted a proposal for a Cyber Security Act to implement the Directive, which is currently being discussed by Parliament. However, it is likely that the Act will not yet be in force on 18.10., when the NIS2 Directive will start to apply throughout the EU. A situation in which a directive adopted at EU level is in force but national law is not in force is challenging from the perspective of companies falling within the scope of the directive and creates uncertainty in the field of operation. It is therefore important that the legislation enacted in Finland enters into force as soon as possible. The cyber industry has published an application guide to support the companies covered, an updated version of which will be published once the law is finally adopted. Experts from dozens of cybersecurity expert companies have been involved in the preparation of the guide, which has enabled the utilisation of wide-ranging excellence and different experiences.

Last, but possibly the most significant, legislative preparation is the EU's Cyber Resilience Act (CRA). It is a massively broad EU regulation that sets minimum data security requirements for almost all hardware and software offered on the EU market. In other words, it is about digital product safety during the life cycle of products. The regulation aims to ensure that products are placed on the market (including from third countries) and kept safe for use by the manufacturer. Product safety means higher information security and is a necessary element in the digital operating environment. The Council of the EU and the European Parliament reached an agreement on the content of the regulation in November 2023 and it is expected to be finalised by the end of 2024. The regulation will enter into force gradually over a three-year transition period by 2027.

At best, ambitious new regulations can make Europeans' digital lives significantly safer and more functional and become global standards that are also respected in other parts of the world. However, this requires massive investments to ensure uniform and successful implementation of regulations in all EU Member States. If implementation is carried out carelessly or suboptimally, it means that important objectives of the regulation will not be achieved. At the same time, companies struggle with increased obligations, administrative burdens and, in the worst case, serious ambiguities in interpretation and other challenges that weaken business conditions. In addition to sufficient efforts, it is essential that the responsible authorities genuinely and actively involve the companies covered by the regulations and their representatives in the work. Especially taken together, the new regulations form such a significant entity that it is not possible to manage it by the authorities alone. Companies and the third sector need to be involved in devising the best means of implementation and producing the necessary new products and services.

In particular, successful national implementation of the Cyber Resilience Act would enable competitive advantages for Finnish companies. This requires that the Ministry of Transport and Communications, in cooperation with The Finnish Transport and Communications Agency, Traficom, creates clearer incentives for companies suitable as assessment bodies for products requiring third-party approval and proactively approves them to a sufficient extent. The assessment bodies will particularly benefit Finnish export companies, which would be able to access the EU's internal market more reliably and quickly than their international competitors. Prompt and extensive approval of organisations would also enable assessment service companies to offer services to hardware and software manufacturers and importers operating throughout the EU. This would strengthen the cybersecurity industry ecosystem operating in Finland, as well as increase employment and tax revenue. The risk-based conformity assessment shall not become a barrier to market entry for domestic products. More than half of the products of Finland's largest listed companies and a huge number of SMEs are subject to new technical requirements as a result of the regulation. If there are not enough assessment bodies, the effects on Finnish business and thus on the national economy will be very harmful. Involving stakeholders and taking their needs into account in different areas of implementation significantly strengthens the prerequisites for success.

The Finnish Transport and Communications Agency Traficom plays a key role in implementing the national implementation of new EU regulations. As fiscal adjustment needs increase, the tasks of Traficom and other relevant agencies need to be assessed and specified, and tasks related to the implementation of the Cyber Resilience Act and other EU regulations must be prioritised in the allocation of resources allocated to them. Activities related to the national implementation of EU regulations have significant multiplier effects on the functioning of society and the operating conditions of Finnish business, and thus on employment and economic growth. At the Transport and Communications Forum held in September, Minister of Transport and Communications Lulu Ranne promised that the implementation of the new EU regulation would be implemented in a way that supports economic growth. The idea from the point of view of the business community is very much to be welcomed, but at the same time it must be borne in mind that implementation that supports growth requires real attention to be paid to it.

The cyber industry has been actively involved at all stages of the lifecycle of new EU legislation. Together with our umbrella organisation Technology Industries of Finland, we actively contributed to the preparation of the NIS2 Directive and the Cyber Resilience Act, as well as the Artificial Intelligence Regulation and the Data Regulation, especially for the European Commission, the European Parliament and the Government. Now we are actively cooperating with the authorities to support the national implementation of regulations and mobilising our association's member organisations to participate in this work. We are happy to advise our member organisations and partners on questions related to new EU regulations and provide information on the possibilities related to their implementation. In this work, we also have access to the resources of Technology Industries of Finland. ■


**PETER SUND**

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



**RISTO RAJALA**

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

# FROM HUNCHES TO FORECASTS: COMBINING MACHINE AND HUMAN INTELLIGENCE FOR CYBER-INFORMATION SENSEMAKING

// Chris Bronk

**ABSTRACT:** Hybrid warfare operations embrace an "anything that gets results" strategy, including significant information operations. Western democracies need to better understand the information operations that are undertaken against them. This will need to involve more rigorous observation, monitoring and measurement of malign political campaigns undertaken against them via the internet.

**BOTTOM LINE UPFRONT:** Theories of information power and influence can be tested and optimized with advancing technology for the observation of internet dataflows and other related phenomena. This activity needs to be undertaken, at scale and in the open, to better protect democratic societies from malign influence campaigns. There will be ancillary gains in intelligence collection and analysis from such activity.

**PROBLEM STATEMENT:** How can hybrid information influence on conflict operations be detected, tracked and countered?

**SO WHAT?** The most open societies are probably the most vulnerable to data manipulation and information operations. The community of democratic states must erect defences against malign information influence delivered through cyberspace.

## A TRANSFORMATION IN INFORMATION POWER

More than eighty years ago the British diplomat, journalist and academic Edward Hallett Carr declared in his The Twenty Years' Crisis that power could be exerted in three areas – military, economic and information.[1] Substituting his term soft power for power over opinion, Nye produced a similar assessment six decades later.[2] While practitioners and scholars may agree that information power is important, borrowing from Simon, one must ask, "to what extent have the operational tools of observation and measurement been provided us?"[3] The task at hand for scholars and practitioners of the geopolitical information environment is to identify how burgeoning sources of information may be processed and analysed by the novel computational methods referred to as artificial intelligence (AI).

## WHAT MAKES FOR INFORMATION AWARENESS IN HYBRID CONFLICT?

Resilient, accurate situational awareness of hybrid threats depends on observation and measurement in each sub-area in the hybrid arena, which blends "the lethality of state conflict with the fanatical and protracted fervour of irregular warfare."[4] Such observation translates to monitoring many different types of activity undertaken by an adversary. Governments and other actors have created all manner of observation and measurement capacities, from social media and banking systems to computer networks and reconnaissance satellites. This new form of interstate conflict is set apart from our fading memories of the Cold War in that where data were once difficult to find, there is often now an overabundance of them.[5] New issues arise, however. Data of sufficient quality may be used to measure phenomena, and that measurement is a key step to situational awareness.[6]

Computing has given humankind a greater capacity to assign quantitative measures to all manner of phenomena. Mobile computing devices provide sensor data from images to geolocation.[7] At the outset of the February 2022 invasion of Ukraine, images of military action, largely taken from mobile devices, flooded social media.[8] Open-source intelligence (OSINT) analysts, mostly amateurs, sifted through online video and images of combat to generate a picture of the military action.[9]

As for combining inputs at a strategic level and then translating them to operational action, the most important issues will be the accuracy of the information inputs from all sources and the timeliness of their analysis. An example of success in this area is the Ukrainian missile attack on the port of Berdiansk in March 2022.[10] Russia released a propaganda video of its operations at the seaport that allowed accurate Ukrainian targeting of Russian amphibious ships there. The Ukrainian missile attack then sank one of the ships and badly damaged two others.[11] This form of OSINT may be highly useful; its incorporation into a rapid, task-oriented intelligence analysis enterprise, however, presents challenges – not least the potential for disinformation by a wary enemy.

The intelligence picture available to government, industry and individuals today differs greatly from what it was during the last period of major power competition, which ended with the demise of the Soviet Union.[12] The enormous technological advances in information and computing technologies (ICTs) have completely overhauled the craft of intelligence. Foreign agents can be recruited in chat rooms rather than back alleys. Overhead intelligence, once the province of superpowers, is now available commercially by download over the internet. There is no need to break open filing cabinets when computers may be electronically compromised, and contents pilfered by actors half a world away. A bonanza of sorts exists for the collectors of intelligence. However, for those from whom intelligence is being collected an acknowledgement of the huge value of their "digital exhaust"[13] comes only after those data are translated to

action – from online censorship to artillery bombardment. The communications revolution represents a double-edged sword for high-technology societies and their high-technology militaries.

There is no question that mobile smartphones, which perform the role of everything from calculators and cameras to media studios and flashlights, have made an enormous impact on humanity.[14] The number of cell phone subscriptions surpassed the global population sometime between 2015 and 2020.[15] Sweden's Ericsson, the builder of the technological infrastructure that runs mobile communication, contends that some 60 per cent of the planet's population have "äppärät" smartphones.[16] Between 2023 and 2024 the amount of data travelling between these devices and other pieces of ICT infrastructure grew by 25 per cent.[17]

On the downside these devices may be tracked, monitored and targeted by technologies that scan the electromagnetic spectrum and inspect dataflows on backbone networks and hacking tools compromising apps and operating system software. On the battlefields of the Russo-Ukrainian War they have been shown to be a huge liability. Presence on cell phone networks along the frontlines of that conflict and others is a common trigger for attack – and has been for more than a decade.[18] That Russian small unit commanders tack mobile phones to the walls of bunkers if they are found among frontline troops, as they did in one viral instance, is solid proof of the vulnerability the technology opens to military units.

Picture: A Russian soldier nails confiscated cell phones to a post in 2024. Source: @clashreport, x.com.

One of the more surprising developments of the Russo-Ukraine War is the utility of commercial internet and cellular technology on the battlefield. That artillery fires are called in via a Starlink satellite modem is but one of the unforeseen developments of that conflict. Keeping tabs on the activities identified as hybrid or "grey zone" conflicts incorporates information from multiple platforms and systems.[19] Included in an ontology of hybrid conflict are: propaganda operations, principally undertaken online; official declarations and press reports; computer network attack and defence activity; information about military movements and exercises; and economic data (i.e. buying up fuels to prepare for war or manipulating markets to create an asymmetric advantage). As it was in the early days of the Cold War, the goal for states facing acute security issues and responsibilities is to avoid surprise.[20] Its avoidance today means that capacity must grow in analysing the flood of data we call intelligence.

## MEASURING HYBRID INFLUENCE AND ACTION

At a time when the hyperbole regarding artificial intelligence (AI) could hardly be stronger, the human capacity to understand information remains constrained by attention and time. It would take a single person 200,000 years to read the amount of information on the world wide web (www) alone. The good news for prospective hybrid warfare analysts is that not everything needs to be read, and what does can be accomplished by organizations of professionals. Analytics teams can monitor variables relevant to information operations, but the question is how.[21] The answer is tripartite, involving (a) identifying key variables; (b) baselining of what we may call "normal" activity; and (c) the weights of different variables in a machine learning algorithm for processing collected data. A framework may emerge from this for observing change in the exertion of information power.

Understanding hybrid conflict involves the incorporation of manifold areas of knowledge. Much of this is encompassed in what contemporary Western military theorists call the information environment.[22] Setting bounds to that environment is daunting. It is large, much like the physical environment in which it is constructed. Much of the information now exchanged and absorbed by people is digital. This indicates enormous streams and repositories of data. The challenge lies in locating those sources that may better illuminate the exertion of power in the international system. Scholarship on the information dimension of international relations has been approached by methods of news analysis,[23] public declaration,[24] leadership analysis and related political psychology,[25] and for some time now internet communications and interactions.[26] Thanks to the continued

durability of Moore's Law in the growth of computing power, the mechanisms for enquiry in these areas may be re-engineered in light of technological advances.[27]

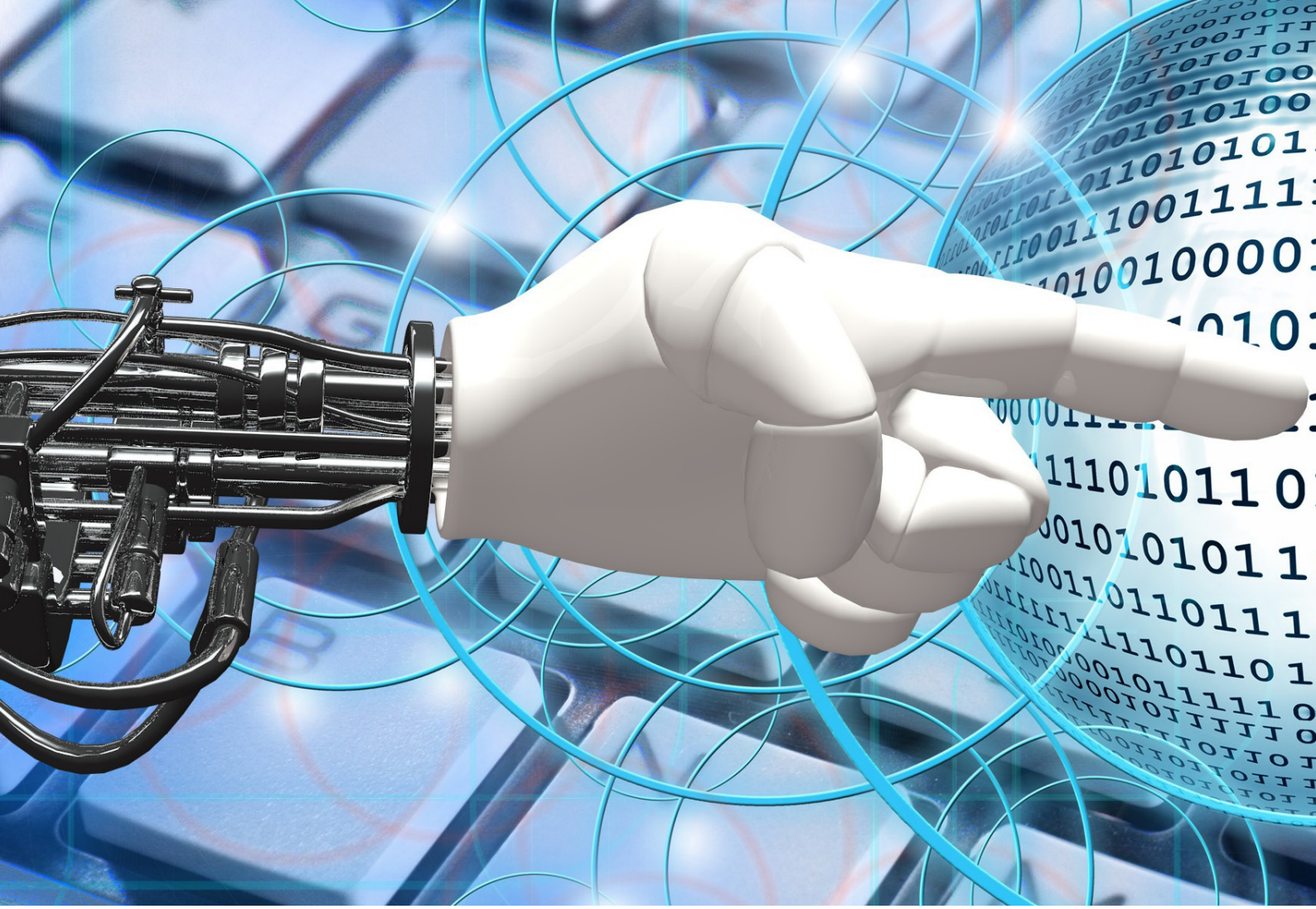
In the information environment of hybrid warfare, a bridge must be constructed between technical capacity and social response. Advertising may offer a shortcut to valuing information power in international competition and conflict.[28] Technology has revolutionized the advertising industry. With the arrival of ubiquitous computing, advertisements delivered by internet companies such as Alphabet (Google) and Meta (Facebook) target individuals rather than audiences.[29] Spending on political advertising in the US is projected to reach almost $3.5 billion in the 2024 election cycle, while traditional advertising spending (TV, radio, print, etc.) is still far more, at some $7.9 billion. The total amount, some $12 billion, represents an increase of nearly a third from the 2020 election cycle. Most of that growth is in what the advertising industry calls "digital",[30] which is a pathway to discovering information power variables.

The largest growth area for political advertising spending is in what the advertising industry calls connected television. Connected TV is video delivered by the internet.[31] Services from Alphabet, Amazon, Netflix and traditional media companies like Disney deliver these advertisements to viewers. They appear in a burgeoning flood of video, as some 20 days' worth of video is uploaded to Alphabet's YouTube service every minute. In this exponentially growing video archive, propagandists deliver their messages to the public abroad.[32] Interestingly, the Russian government recently blocked its citizens from accessing the service.[33] It appears likely that both video content and the advertisements surrounding it are a potential threat to some states. These categories of digital data should also be tracked by those who observe hybrid conflict.

On X (formerly Twitter), Telegram and Alphabet's Instagram many variables, including the metadata produced by those platforms, must be followed by practitioners of active measures.[34] Government officials and political candidates make use of these internet platforms to communicate their messages.[35] Propagandists are somewhat less upfront about how they spread their narrative views but work with the same technologies.[36] Where once practitioners of active measures covertly published magazines and newsletters, they now create online news and opinions,[37] often with assistance from Large Language Model (LLM) AI models.[38] Situational awareness for hybrid conflict translates to effective monitoring of sources of information designed to influence beliefs. Such activity will probably need to be undertaken for the foreseeable future. Information power still appears to be relevant.

## HOW DOES INFLUENCE WORK IN THE HYBRID CONTEST?

To understand whether influence operations work, consider the example of Russia's attempts to isolate Ukraine and deprive it of Western support. Until the US Congress voted to approve a major round of assistance to Ukraine in April 2020, Russian propaganda held up US legislative action on the provision of military aid to Ukraine for months. A recent Breitbart headline, "Exclusive: [House Speaker] Johnson's top policy advisor is former lobbyist… Clients have corporate interest in Ukraine War", exemplifies information operations in which pro-Russia actions are camouflaged in the anti-corporate narrative.[39] Sacked Fox News commentator Tucker Carlson interviewed Vladimir Putin in Russia and lingered to film segments in which he called Moscow "much nicer than any city in my country".[40] One long-serving Republican member of the US Congress



chastised his own caucus for introducing Russian propaganda talking points as fact to the chamber's deliberations.[41]

Hybrid conflict-oriented propaganda also targets both the national politics and militaries of targeted countries.[42] What this means in practice is their ideological compatibility with missions that may be subject to tremendous political propaganda. False reports of violence by German soldiers serving in Lithuania may be but the tip of the iceberg in the anti-NATO digital propaganda undertaken by Russia.[43] Perhaps the best indicator of its effectiveness is the presence of neo-fascistic elements in NATO militaries and their willingness to work against their own services due to malign foreign information influence propagated across cyberspace.

Although not a military conflict, the covid-19 pandemic likewise opened the doors for propagandists, including those in the US, to manipulate publics online.[44] False narratives fooled the naive and intellectually impressionable. In some cases the cost was their lives. Hybrid conflict indicators abound in the information environment, but their presence does not necessarily provide a forecast of future military conflict or covert action. Connecting the dots on information operations in a conflict that may pass from the "grey zone" to significant hostilities is required for early warning and efforts at peace. That also means that the mere bellicosity of rhetoric between two states does not necessarily add up to open conflict. Now toned down, the war of words between Japan and South Korea spoke to an old animosity but not a renewed conflict.

## AI'S ROLE IN GRASPING UNDERSTANDING IN A SEA OF DATA

ICTs have transformed society, particularly through the rapid proliferation of information. Perhaps the most important observation in the preparation of this essay was an oft-repeated belief that AI answers all questions, removing the need for critical thinking.[45] This could have devastating effects as we learn more about how AI performance can be biased, and how that bias can be influenced.[46]

A tremendous computational capacity for the sensemaking of digital information is at hand. The technologies to process information can be incredibly useful in bringing order to the chaos of the information environment.[47] For example, BERT, a computational-linguistic tool, can be trained to detect online propaganda through its ever-evolving linguistic model.[48] For every advance in detecting information operations, however, the propagandists will also innovate. This is the nature of technologically infused statecraft. When divided into sides, players in the international system attempt to leverage innovation for comparative advantage.

The information components of hybrid conflict can be found, and this can partly be undertaken by computers. That said, AI is no panacea. There is perhaps too much talk about AI by those who may not understand how the technology works today or will evolve. However, the evolution of the neural network machine learning process we call AI is advancing consistently. The head of Google's Deep Mind division, the centre for the company's AI research and development, has asserted recently that these advances will continue. He observes: "In recent years, I think machine learning has really changed our expectations of what we think of computers being able to do. If you think back 10 or 15 years ago, speech recognition kind of worked, but it wasn't really seamless – it made lots of errors. Computers didn't really understand images from the pixel level of what was in that image. There was a bunch of work in natural language processing, but it wasn't really a deep understanding of language concepts and multilingual data. But I think *we've moved from that stage to one where you actually expect computers to be able to see and perceive the world around us in a much better way than they were able to 10 years ago* [author's italics]."[49]

While Dean sees tremendous advances in computer reasoning, the data for understanding information influence or other hybrid warfare tactics will require sophisticated models. One approach is to simulate society at scale. One research group envisages the employment of High-Definition Cognitive Models representing the mindset of specific individuals.[50] The challenge with such an approach is to capture the heterodox nature of a population and understand how AI approximation may yield useful observations. Computing advances will continue, but the greater challenge may be structuring and weighting data to construct useful analytical tools. That process, let alone hybrid warfare, remains relatively immature as applied to international relations.

## GROWING CIVILIAN AND DIPLOMATIC INSTITUTIONS

Hybrid conflict embraces a repertoire of actions that can produce a maximum effect while simultaneously managing escalatory dynamics. The governments of the West's democracies employ diplomatic, intelligence and military capabilities to maintain peace and offer early warning in a way not seen before the paired catastrophes of two world wars. In the decades since 1945 those organizations have adapted to manifold threats, from denial and disinformation operations to thermonuclear warfare. Assuring security has required the contributions of many actors availing themselves of new technology and tradecraft for necessary adaptation to the methods of intelligent and motivated adversaries.

That adaptation also extends to alterations in the proverbial "rules of the game" in international relations. Deepfakes, kinetic cyberattacks and transnational criminal-terror syndicates are all realities of the contemporary security environment that would have been labelled science fiction a few decades ago. In addition to new actors and actions, the conflict now plays out on a deeply globalized geographic information tableau upon which advantage is sought while keeping escalation in check, and a significant challenge remains in directing the attention of computer algorithms to both find and analyse them. Hostile and aggressive states use the tools they have at hand. North Korea, for example, has learned how to employ cyber tools to perpetrate the first heist of a national reserve bank.[51] The capacity for innovation in a digitally interconnected world is a source of regular surprise for the community of states seeking a norms-based international order that promotes shared interests and collective security. Staying apprised of that innovation, undertaken by a growing club of authoritarian regimes increasingly willing to collaborate, must be a priority.

If there is a defining attribute of our time, it is that societies can cope with torrents of information to make sense of the world they inhabit. The information environment grows exponentially. Tracking what goes on within it will be the job of practitioners in many disciplines who can cooperate in making sense of the perception we call security. Journalists, academics and concerned citizens will be at the vanguard of discovery for hybrid warfare information operations. In the Global West governments should not get a pass just because these actors are present and capable, however. While military alliances are built on the cooperation of armed forces, Western democracies would be wise to grow civilian and diplomatic institutions for hybrid conflict in the digital domain.

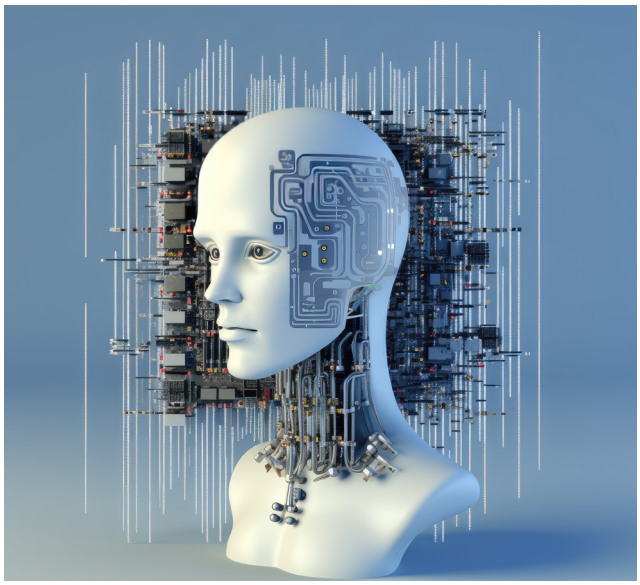
What this will mean is probably a further erosion of institutional or organizational silos related to security. Police, spies, soldiers, corporations and interested citizens of all stripes will contribute to sensemaking in a world marked by hybrid conflicts. How that collaboration will function is very much a work in the earliest phases of progress. Perhaps the most important question for identifying the machinations of hybrid warfare is what it will cost those who wish to deter it in both blood and treasure. ■


**CHRIS BRONK**

Chris Bronk PhD is an associate professor at the University of Houston's Hobby School of Public Affairs. He studies the intersection of information and computing technology with international relations. The views contained in this article are the author's alone and do not represent the views of the University of Houston or the State of Texas.

## ENDNOTES


[1] Edward Hallett Carr, The Twenty Years' Crisis, 1919–1939: Reissued with a new preface from Michael Cox (Springer, 2016).
[2] Joseph S. Nye, The Future of Power, (Public Affairs, 2011).
[3] Herbert A. Simon, 'Notes on the observation and measurement of political power', The Journal of Politics Volume 15, Issue 4 (1953): 500–516.
[4] Sub-areas of hybrid conflict can include cyber activity, terrorism, information operations, international crime, and economic activity. Frank G. Hoffman, 'Hybrid warfare and challenges', in Strategic Studies, 329–337. (Routledge, 2014).
[5] Margret S. MacDonald and Anthony G. Oettinger, 'Information overload', Harvard International Review Volume 24, Issue 3 (2002): 44.
[6] Erhard Rahm and Hong Hai Do, 'Data cleaning: Problems and current approaches', IEEE Data Engineering Bulletin Volume 23, Issue 4 (2000): 3–13.
[7] Zheng Xu, Lin Mei, Kim-Kwang Raymond Choo, Zhihan Lv, Chuanping Hu, Xiangfeng Luo, and Yunhuai Liu, 'Mobile crowd sensing of human-like intelligence using social sensors: A survey', Neurocomputing 279 (2018): 3–10.
[8] Aaron F. Brantly, 'Ukraine War OSINT Analysis: A Collaborative Student Report' (2023).
[9] Generating intelligence from social media was defined almost a decade ago. OSINT has been discussed significantly since the 1990s. Laura K. Donohue, 'The dawn of social intelligence (SOCINT)', Drake Law Review Volume 63 (2015): 1061.
[10] Chris Bronk, Gabriel Collins, and Dan S. Wallach, 'The Ukrainian Information and Cyber War', The Cyber Defense Review Volume 8, Issue 3 (2023): 33–50.
[11] Brent D. Sadler, 'Applying Lessons of the Naval War in Ukraine for a Potential War with China', Backgrounder 3743 (2023): 1–13.
[12] Alex Roland and Philip Shiman, Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983–1993 (MIT Press, 2002).
[13] Ronald J. Deibert, Reset: Reclaiming the Internet for Civil Society (House of Anansi, 2020).
[14] Muhammad Sarwar and Tariq Rahim Soomro, 'Impact of smartphones on society', European Journal of Scientific Research Volume 98, Issue 2 (2013): 216–226.
[15] https://www.weforum.org/agenda/2023/04/charted-there-are-more-phones-than-people-in-the-world/.
[16] The term "äppärät" is borrowed from Gary Shteyngart's Super Sad True Love Story, a 2011 novel set in a dystopian near future where mobile devices were all-consuming of human attention. Sounds crazy. Gary Shteyngart, Super Sad True Love Story: A Novel. (Random House Trade Paperbacks, 2011).
[17] This data traffic growth of 25 per cent a year is a staggering statistic and has held true for more than a decade. Fredrik Jejdling, Ericsson Mobility Report 2024. June 2024.
[18] Chris Bronk and Gregory S. Anderson, 'Encounter battle: Engaging ISIL in cyberspace', The Cyber Defense Review Volume 2, Issue 1 (2017): 93–108.
[19] Michael J. Mazarr, 'Mastering the gray zone: Understanding a changing era of conflict', US Army War College (2015).
[20] Roberta Wohlstetter, Pearl Harbor: Warning and Decision. (Stanford University Press, 1962).
[21] The value of AI technologies for analytic teamwork is in its earliest phases. Lauro Snidaro, 'ChatGPT Act as an Intelligence Officer', In 2023 IEEE International Workshop on Technologies for Defense and Security (TechDefense), 449–454. IEEE, 2023.
[22] Michelangelo Conoscenti, 'The Military's Approach to the Information Environment', in The Routledge Handbook of Discourse and Disinformation (Routledge, 2023), 218–238.
[23] Kalev Leetaru and Philip A. Schrodt, 'Gdelt: Global data on events, location, and tone, 1979–2012', in ISA annual convention, Volume 2, Issue 4: 1–49. Citeseer, 2013.
[24] Gavan Duffy and Brian Frederking, 'Changing the rules: A speech act analysis of the end of the Cold War', International Studies Quarterly, Volume 53, Issue 2 (2009): 325–347.
[25] Margaret G. Hermann and Charles W. Kegley Jr., 'Rethinking democracy and international peace: Perspectives from political psychology', International Studies Quarterly Volume 39, Issue 4 (1995): 511–533.
[26] Charli Carpenter and Daniel W. Drezner, 'International Relations 2.0: The implications of new media for an old profession', International Studies Perspectives, Volume 11, Issue 3 (2010): 255–272.
[27] Mark S. Lundstrom and Muhammad A. Alam, 'Moore's law: The journey ahead', Science Volume 378, Issue 6621 (2022): 722–723.
[28] Garrett A. Johnson, Randall A. Lewis, and David H. Reiley, 'When less is more: Data and power in advertising experiments', Marketing Science Volume 36, Issue 1 (2017): 43–53.
[29] Ritam Dutt, Ashok Deb, and Emilio Ferrara, '"Senator, We Sell Ads": Analysis of the 2016 Russian Facebook Ads Campaign', in Advances in Data Science: Third International Conference on Intelligent Information Technologies, ICIIT 2018, Chennai, India, 11–14 December 2018, Proceedings 3, 151–168. Springer Singapore, 2019.
[30] Trade press publications can offer some interesting insights. The $12 billion ad spend is an amount roughly the size of Guyana's GDP. '2024 Political Ad Spending Will Jump Nearly 30% vs. 2020', EMarketer, 11 January, 2024, https://www.emarketer.com/press-releases/2024-political-ad-spending-will-jump-nearly-30-vs-2020/.
[31] Paul Murschetz, 'Connected television: Media convergence, industry structure, and corporate strategies', Annals of the International Communication Association Volume 40, Issue 1 (2016): 69–93.
[32] Robert W. Orttung and Elizabeth Nelson, 'Russia Today's Strategy and Effectiveness on YouTube', Post-Soviet Affairs Volume 35, Issue 2 (2019): 77–92.
[33] Alexander Marrow and Gleb Stolyarov, 'YouTube slowdown in Russia darkens freedom of speech outlook', Reuters. 8 August 2024. YouTube was blocked by China years ago.
[34] Mylynn Felt, 'Social media and the social sciences: How researchers employ Big Data analytics', Big Data & Society Volume 3, Issue 1 (2016): 2053951716645828.
[35] Jason Gainous and Kevin M. Wagner, Tweeting to Power: The Social Media Revolution in American Politics (Oxford University Press, 2014).
[36] Yevgeniy Golovchenko, Cody Buntain, Gregory Eady, Megan A. Brown, and Joshua A. Tucker, 'Cross-platform state propaganda: Russian trolls on Twitter and YouTube during the 2016 US Presidential Election', The International Journal of Press/Politics Volume 25, Issue 3 (2020): 357–389.
[37] Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux, 2020.
[38] Paweł Golik, Arkadiusz Modzelewski, and Aleksander Jochym, 'DSHacker at CheckThat! 2024: LLMs and BERT for Check-Worthy Claims Detection with Propaganda Co-occurrence Analysis', (2024).
[39] Wendell Husebø and Matthew Boyle, 'Exclusive – Mike Johnson's top policy advisor is former lobbyist: Clients have interest in Ukraine War', Breitbart, 17 April, 2024.
[40] Dominick Mastrangelo, 'Tucker Carlson: Moscow "so much nicer than any city in my country"', The Hill, 13 February, 2024.
[41] Julia Ioffe, 'McCaul to Action', Puck, 2 April, 2024, https://puck.news/ukraine-aid-q-and-a-rep-mccaul-on-republican-support-for-bill/.
[42] Christopher Paul and Miriam Matthews, 'The Russian "firehose of falsehood" propaganda model', Rand Corporation Volume 2, Issue 7 (2016): 1–10.
[43] 'Fake news campaign targets German Army', DW. 16 February, 2017.
[44] Chris Bing and Joel Schectman, 'Special Report: How U.S. Taxpayers Funded a "Global Propaganda" Program to Push Covid-19 Vaccine Abroad', Reuters, 25 July, 2023.
[45] Claire Su-Yeon Park, Haejoong Kım, and Sangmin Lee, 'Do less teaching, do more coaching: Toward critical thinking for ethical applications of artificial intelligence', Journal of Learning and Teaching in Digital Age Volume 6, Issue 2 (2021): 97–100.
[46] Reva Schwartz, Apostol Vassilev, Kristen Greene, Lori Perine, Andrew Burt, and Patrick Hall, Towards a Standard for Identifying and Managing Bias in Aartificial Intelligence. Volume 3, US Department of Commerce, National Institute of Standards and Technology, 2022.
[47] Stephen L. Dorton and Robert A. Hall, 'Collaborative human-AI sensemaking for intelligence analysis', in International Conference on Human-Computer Interaction (Cham: Springer International Publishing, 2021), 185–201,.
[48] For more information about BERT: Mikhail V. Koroteev, 'BERT: A review of applications in natural language processing and understanding', arXiv preprint arXiv:2103.11943 (2021).
[49] Jeff Dean, 'Exciting Trends in Machine Learning', (Lecture), Rice University, Houston, TX, 13 February. 2024.
[50] Michael Bernard, George Backus, Matthew Glickman, Charles Gieseler, and Russel Waymire, 'Modeling Populations of Interest in Order to Simulate Cultural Response to Influence Activities', in Social Computing and Behavioral Modeling, 1–8. )Springer US, 2009).
[51] Seongjun Park, 'Evading, Hacking & Laundering for Nukes: North Korea's Financial Cybercrimes & the Missing Silver Bullet for Countering Them', Fordham International Law Journal Volume 45 (2021): 675.

# DEFENDING FREE SPEECH WITH FREE CHOICE: TOWARDS TECHNOLOGY-DRIVEN, HUMAN-CENTRED, ENDPOINT SOLUTIONS FOR SOCIETY AS A WHOLE

// Maria Papadaki

**ABSTRACT:** Cognitive warfare and especially disinformation now rely heavily on social media platforms, cybertechnologies and AI, with the aim of creating confusion, societal polarization, mistrust, anger, and hatred against governments, organizations, communities or opposing individuals. While disinformation is a global problem, early defences based on censorship also threaten core Western values such as freedom of speech and democracy. Unsurprisingly, when surveyed, EU citizens overwhelmingly consider disinformation a threat to democracy.

**PROBLEM STATEMENT:** How can cybersecurity and AI serve democratic values and human rights for cognitive threat support while seeking to introduce the need for transparent, customizable and cognitive endpoint support tools?

**BOTTOM LINE UPFRONT:** To explore defence options that respect democratic values and human rights, user-centric functionality that can maximize support and minimize human errors, and that is accompanied by the freedom of choice to apply it at an individual level, is necessary.

**SO WHAT?:** The need to complement existing defences at endpoints is analysed, and indicative functionality is outlined and grouped according to the different response objectives – namely, support and education, threat surface reduction, detection and response, and situational awareness. A conceptual architecture, requirements analysis, use cases and proof-of-concept functionality could extend this work to illustrate its key points.

## THE RISE OF SOCIAL MEDIA AND DEMAGOGUES

The rise of demagogues through democracy is not a new phenomenon, nor are their attempts to exploit new communication media to spread propaganda, manipulate the public and eventually lead them to tyranny. Since the inception of democracy Plato has warned of the danger of demagogues using democracy's freedoms against itself. In modern times social media, as a new communication medium, invites many parallels to be drawn with historical examples, albeit now with global reach and amplified consequences.

While studies agree that mainstream media such as newspapers, radio and television remain the most important communication platforms, they also acknowledge the growing popularity of social media as a news and media outlet, especially among younger demographics. As the Flash Eurobarometer 536 survey reveals, a quarter of EU citizens, particularly those among the 15–24 age group,[1] have found data and statistics about their country or Europe on social media. Similarly, almost two in five respondents to the 2023 Media & News Survey (and three in five 15–24-year-olds) used social media to access news.[2] The percentage was even higher in the UK, with almost half of UK adult respondents and 71 per cent of 16–24-year-olds using social media for news.[3] Notably, the rise of TikTok as a news media platform has been steep, with ten per cent of those aged over 16 receiving news through it in 2023, up from one per cent in 2020.[4]

It is therefore understandable that political parties, organizations and individuals use social media to reach their audiences. However, unlike mainstream media, where the same content is transparently available to all who choose to access it, social media content is curated, microtargeted, promoted or suppressed by opaque platform algorithms, often irrespective of user choice.[5] This limits accountability and opens the door for demagogues seeking to use disinformation to manipulate and polarize. Despite the challenges of auditing, disinformation tracking software such as that developed by researchers at Trollrensics has emerged. It has found coordinated networks used to flood social networks with disinformation during the 2024 European elections, particularly in the interests of far-right parties. An analysis of 2.3 million posts in France, Germany, Italy and the Netherlands revealed 50,000 accounts spreading disinformation: one in five posts mentioned far-right French politician Éric Zemmour; and one in ten German posts about Alternative für Deutschland came from disinformation accounts.[6] With three billion people across the world expected to vote in elections in 2024 and 2025 it is perhaps unsurprising that the World Economic Forum (WEF) has identified disinformation as the most severe global risk over the next two years. The WEF also confirms the strong links between disinformation and societal and political polarization, interstate violence, and the erosion of human rights.[7] Democracy and human rights (including free speech) are particularly important values to Western societies.[8]

## FROM DISINFORMATION TO POLARIZATION AND COGNITIVE WARFARE

In addition to attempting to sway elections in favour of autocratic candidates, the broader role of disinformation in cognitive warfare should be considered. Professor Miller recognizes disinformation and sophisticated psychological manipulation techniques as key features of cognitive warfare.[9] Relying heavily on social media platforms, cybertechnologies and AI, these techniques remain closely interlinked and aim to cause confusion, societal polarization, mistrust, anger and hatred towards Western governments, organizations, communities or opposing individuals.[10] [11] The war in Ukraine has

provided ample examples of the role of disinformation/FIMI in cognitive warfare, and how Ukrainian forces have adapted their defences accordingly.[12]

Arguably, allowing these threats to proliferate could lead to the rise of extremist, far-right and misogynistic movements, which could threaten human rights. Some early indications can be seen in a study by King's College London and Ipsos which showed that younger male participants expressed more negative views of feminism than their older counterparts.[13] Andrew Kaung, a former TikTok analyst, revealed the differences in content recommendations that teenage girls and boys received, irrespective of their choices. Teenage boys were shown violent misogynistic content; girls were shown content related to music or makeup.[14] A further study by NPCC has indicated a notable rise in the number of crimes against women and girls in the UK, which may be linked to the radicalization of men by social media influencers promoting misogyny. The result is that they have since upgraded gender-based crimes to a national threat akin to organized crime and terrorism.[15]

An example of disinformation fuelling violence and extremism was seen after the killing of three children in Southport in the UK in July 2024. Despite the UK authorities publishing the details of the suspect, who was born in the UK, the crime had already been attributed to immigrants through disinformation from foreign-owned websites. The false association between immigration and violent crime has had the unfortunate effect of mobilizing far-right groups that have resorted to attacking immigration support structures across the country. There was a particular focus on Muslim and refugee communities, which led to attempts to incite anger, violence, anxiety and fear across society.[16] [17] It would be premature to attribute this disinformation incident to FIMI actors at the time of writing. Nevertheless, whatever the intention or attribution, its effects were real, and this relationship should be acknowledged.

The 2nd EEAS report on FIMI Threats offers an updated overview of the FIMI ecosystem and reveals its global scale and diverse range of targets. Nearly half the analysed cases targeted countries across the globe, 30 per cent targeted organizations (such as the EU, NATO and Euronews), and nearly 20 per cent targeted individuals, including non-political figures. Furthermore, there seems to be an emerging trend of gender-based and anti-LGBTIQ+ FIMI attacks.[18]

It would be remiss not to consider the potential implications of AI-generated fake content, which the WEF identified as a significant risk for 2024.[19] It is noteworthy that AI-generated audio imitating the voices of politicians has already been utilized in a limited capacity in FIMI cases.[20] The relatively low technological barrier to creating fake content, coupled with the speed and volume at which it can reach individuals, causes concern. Notable examples illustrating its impact, besides character assassination, are deepfake pornography and stock market manipulation. Explicit deepfake images of US

singer Taylor Swift reached millions of views before eventually being removed. Similarly, the promotion of a deepfake image featuring a Pentagon explosion affected US stock markets before the US authorities countered the rumours.[21]

It is possible that this climate of intimidation, polarization and violence, with FIMI in a featured role, will also lead to self-censorship, apathy or coercion if people fear the unwanted consequences of defamation or violence by speaking up. The 2023 Freedom of the Net report indicates that there have been a significant number of attacks against free speech.[22] In three quarters of the countries surveyed individuals have faced legal repercussions for expressing themselves online. In four out of seven countries this has even resulted in physical assault or loss of life.

## CENSORSHIP VS FREE CHOICE

Autocratic regimes have been known to resort to conventional and AI-powered censorship to control the narrative. This can be manifested in several ways, including the blocking of dissenting political, religious or social content, the repression of free speech, and the gradual yet consistent divergence from international human rights conventions.[23] However, censorship could not work in Western societies without eventually opposing their core values and freedoms. The WEF flags the risk that some governments will act too slowly, considering the tradeoff between preventing disinformation and protecting free speech. Meanwhile, others may erode human rights and increase censorship by adopting authoritarian practices.[24]

EU citizens also recognize these risks and overwhelmingly consider disinformation a threat to democracy.[25] Considerable work is underway to gain a deeper understanding of cognitive warfare and develop collaborative multilevel defences.[26] [27] A noteworthy and comprehensive response framework for FIMI threats is the FIMI Toolbox, which is based on a multilevel, collaborative, multidisciplinary, whole-of-society approach.[28]

When considering who has the right and responsibility to decide on the level of protection, there are several stakeholders, each with distinct responsibilities. While it is within the authorities' power to define, regulate and block patterns of illegal activity, there is still scope for further protection, for which individual citizens could be responsible should they choose to utilize them.

## USER SUSCEPTIBILITY TO FAKE STORIES

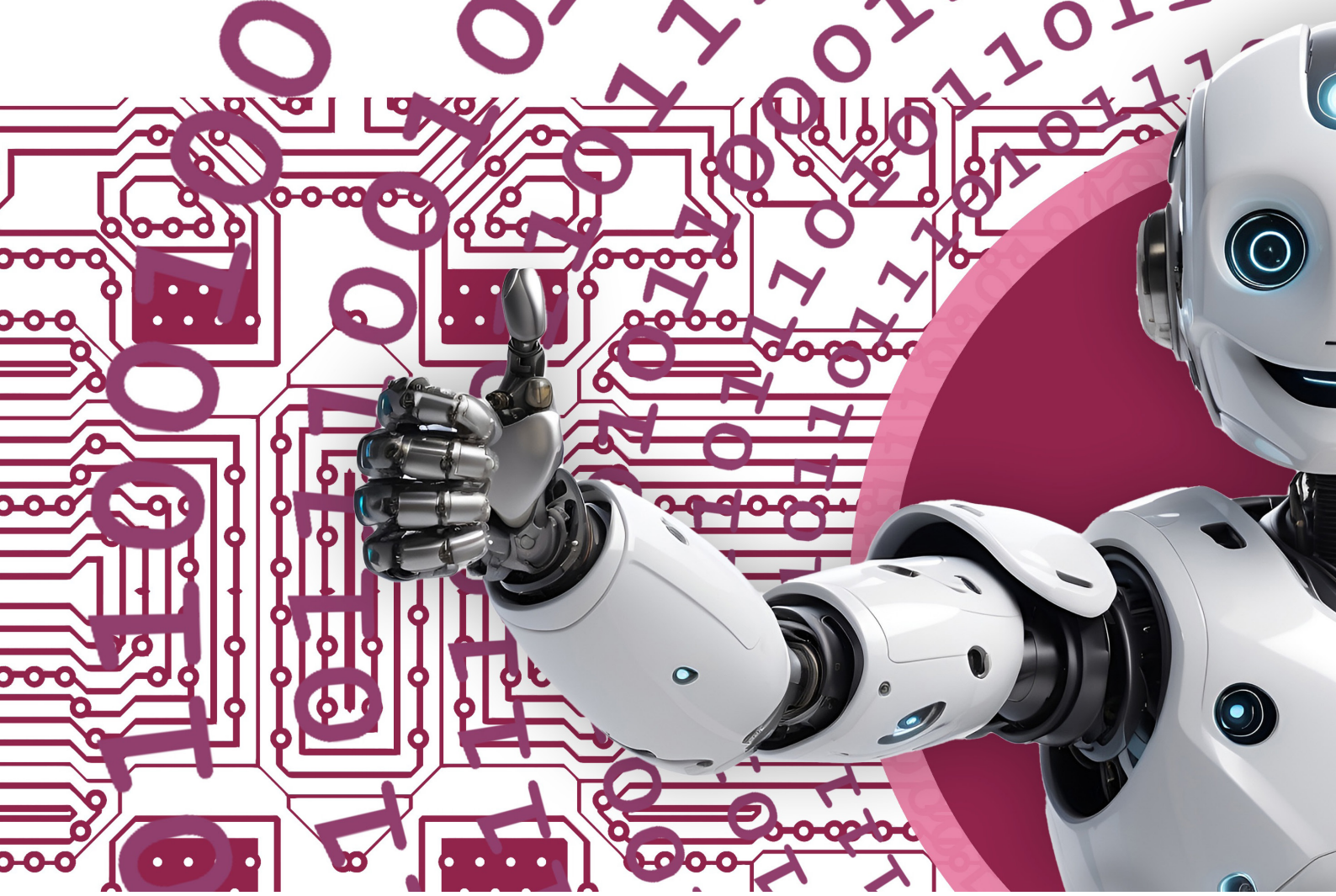
Maertens et al. designed the Misinformation Susceptibility Test (MIST) to understand the scale of human error in identifying fake stories.[29] A survey of approximately 1,500 US citizens found that two out of three news stories could be correctly identified. Younger adults and those relying on social media for their news, however, were less successful.[30] Meanwhile, the Eurobarometer survey, conducted in the EU, indicated that 30 per cent of surveyed EU citizens were not confident that they could recognize disinformation. Confidence decreased with age and increased with level of education.[31] A UK-based Ofcom survey reported similar levels of uncertainty, in which one in three UK internet users were found to be unsure or unaware of the truthfulness of online information. It is also noteworthy that a small subset, six per cent, even believed everything online was unquestionably true.[32] It would be fair to say that error or uncertainty levels are high, particularly when the error rates of another human-related threat, phishing, are considered. While not directly comparable threats or studies, the 2024 Verizon Data Breach Investigations report may still merit consideration. It suggests that phishing click rates ranged from three to ten per cent over the last eight years.[33]

To reduce error rates, it may be helpful to consider the potential impact of education. In the case of phishing Spitzner empirically suggests that initial click rates at the outset of an organization's journey to raising awareness can typically range between 25 and 30 per cent, before eventually dropping to less than five within 18 to 22 months.[34] Awareness and education can highlight cognitive biases and emotional manipulation and encourage critical thinking, allowing humans to spot warning signs of unusual and unexpected attacks. It is also worth acknowledging the wider range of complementary multilayer technological approaches that can contribute to reducing the threat space through automation and ultimately the likelihood of human error by encouraging users to adhere to security norms. These could include email content filtering, blacklisting of known accounts, email origin authentication and validation (in the form of DMARC, DKIM and SPF).

Returning to FIMI and disinformation, it would be useful to consider how AI and human-centric security could help reduce the likelihood of human error (assuming user consent is present). This could involve reducing the threat space, the cognitive load of distinguishing the legitimacy or authenticity of stories, and the technological gap between humans and technological controls.

## DISINFORMATION DETECTION

As a preliminary step towards reducing human error and maximizing user support, this section explores disinformation detection approaches, including sentiment analysis, propagation pattern analysis, origin reputation, provenance, deepfake detection, confirmation bias user profiling and factchecking. Rather than an exhaustive list, this represents a selection of approaches that have informed the options presented in this article.



Early approaches focused on signs of emotionally charged manipulative language or discourse patterns featured in news stories and social media reactions. These approaches involved natural language processing and sentiment analysis of social network content, particularly on X/Twitter.[35]

A prominent indicator worthy of our attention is how these stories spread. Investigations showed that stories aiming to evoke strong reactions were likely to spread faster, or at least differently, than genuine news. Another advantage of identifying anomalous propagation patterns is that it is content-agnostic, making it more easily applicable to multilingual environments. Graph neural networks, or temporal graph networks, can be especially effective at indicating signs of rapidly growing news stories, even adjusting to evolving propagation patterns.[36] [37]

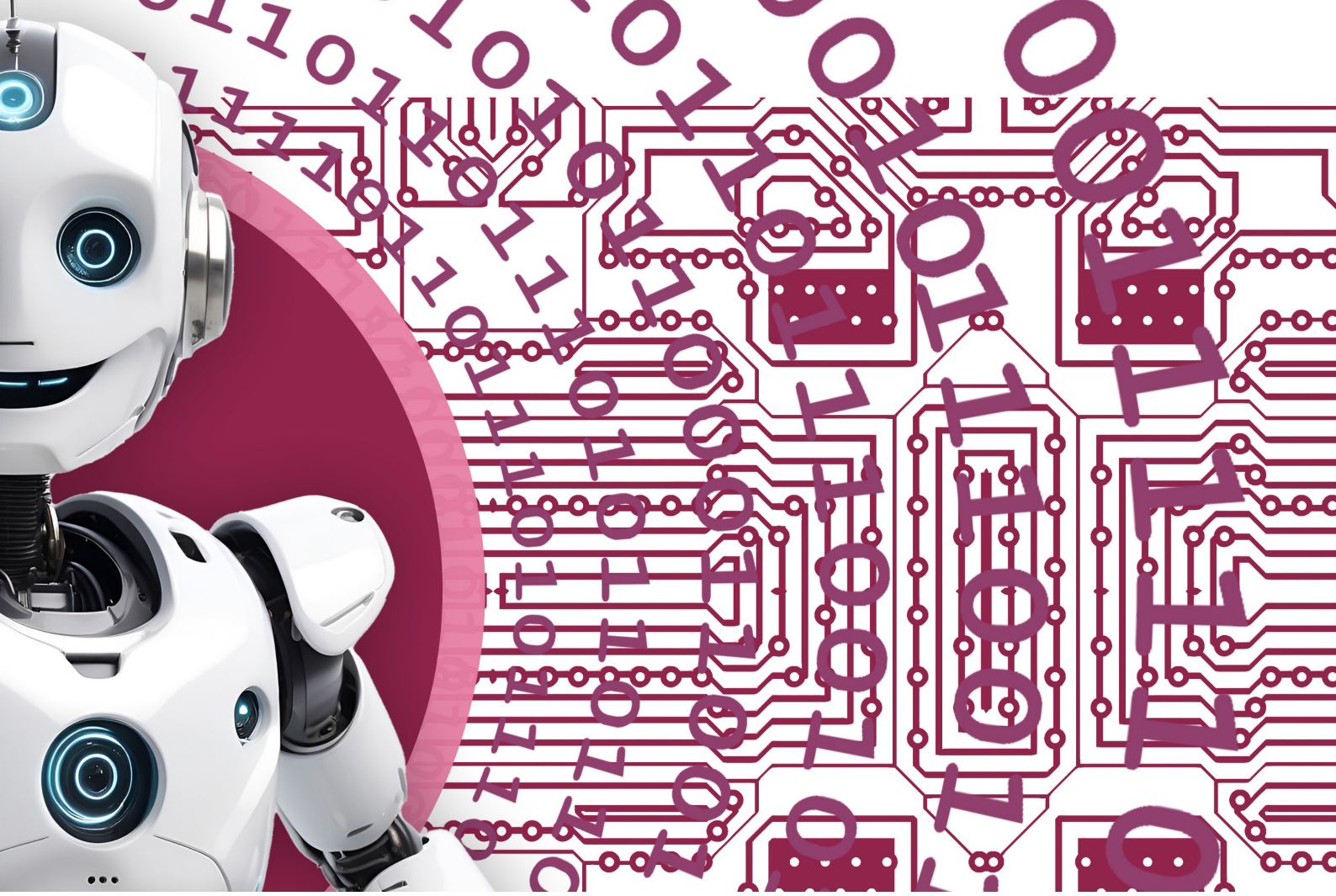
Similarly, it may be possible to identify the anomalous behaviour of bot accounts spreading disinformation as a basis for informing their reputation. Initiatives such as the Coalition for Content Provenance and Authenticity (C2PA) could go even further by cryptographically signing media content to verify its source and editing history. The presence of provenance information, or even its lack, could help improve trust in the authenticity and origin of image, audio or video content.[38]

Deepfake detection aims to identify anomalous effects caused by the editing processes of AI-generated software. In deepfake videos such inconsistencies may be observed in movement or misalignments of key facial points, unusual lighting, shadows and reflections, both within individual frames and sequences. Various methods can be used to detect deepfakes, with deep learning and multi-modal deep learning approaches proving particularly effective.[39]

Another indicator considers the possibility that an individual is more likely to believe and spread misinformation if it already aligns with their existing beliefs, a phenomenon known as confirmation bias. User behaviour profiles of their historical use could therefore help predict individuals who could unwittingly spread misinformation.[40]

The above techniques are designed to detect various patterns of anomalous activity of different entities, which can demonstrate that disinformation detection is indeed possible. There is potential for further improvement by combining these techniques, or even by complementing them with the mapping of the broader characteristics of FIMI and cyber incidents, as defined in the DISARM and ATT&CK frameworks respectively.[41]

Finally, it is important to consider the powerful potential of computer–human teaming methods in the context of factchecking. Communities worldwide collaborate to investigate the accuracy of information based on journalistic standards and to unpack the narrative, intent and potential impact behind disinformation.[42] The



emerging field of Large Language Models (LLMs) and generative AI that have been trained on disinformation datasets incorporate factchecking functionality. These are also important and particularly relevant to end users. Although LLMs show great promise, it would be prudent to await further evidence of their accuracy and resilience to disinformation attacks.

## TOWARDS ENDPOINT SOLUTIONS FOR FIMI THREATS

While cybersecurity principles have inspired the FIMI Toolbox, it is important to acknowledge its stronger sociocognitive elements, which extend beyond technical aspects to encompass a broader range of societal considerations. Its collective response protocols involve an extensive network of relevant stakeholders across society, each with distinct responsibilities, ensuring proportional, adaptive, collective, understandable and effective responses.[43]

Users and citizens have roles and responsibilities as stakeholders to protect their information space and explore how a response paradigm could be provided transparently and democratically. To this end, it is suggested that protection, detection and support functionality are made available at endpoints, where users can freely decide which to enable with the support of customizable default settings. Such user-centric functionality would provide the capacity for the greatest possible support, minimize the risk of human error, and accompany each option with the freedom to enable or disable it at the user level. A group of indicative options for users is outlined below: support and education; threat surface reduction; detection and response; and situational awareness.

## SUPPORT AND EDUCATION

User-initiated support that facilitates the use of factchecking, credibility/reputation scoring, bot detection, disinformation tracking and education could be made available to users through browser extensions, context menu options or LLMs. For example, deepfake audio and video verification functionality (akin to solutions such as Microsoft Video Authenticator, Resemble AI, Sensity AI or WeVerify) could be invoked to verify the credibility of deepfake audio or videos. Simplified reports for factchecking, reverse image searches and content verification could also prove useful. Additionally, access to educational training resources could be facilitated to help users recognize warning signs of disinformation and emotional manipulation, operate suitable tools, understand their output, and select suitable and proportionate response options. Support functionality could also facilitate access to disinformation resources and communities for users who wish to volunteer, connect or report suspected threats.[44]

## THREAT SURFACE REDUCTION

Options for reducing the threat surface could include automated countermeasures for known threats that users would prefer not to see regularly. Several countermeasures could be employed, such as highlighting flagged content, filtering it, replacing it with its authentic alternative or saving it in a secondary alternative location for future review (similar to spam folders for suspected junk email). For example, the default setting might be configured to automatically filter content associated with known disinformation accounts. However, a user might also filter out deepfake political content or content featuring violence and extremism. Another user might want to redirect political content that lacks a verified origin to a secondary location for later review. To avoid undue technological barriers, customizable default recommended settings and user-friendly interfaces that encourage proportionate and appropriate threat reduction would be beneficial, regardless of the social media applications used.

## DETECTION AND RESPONSE

The detection functionality could focus on identifying residual activity and subtler warning signs of novel disinformation threats. Such instances could be reported to the user, escalated to human-computer teams for analysis, or logged locally for future investigation. For example, it might be possible to identify users who are prone to unwittingly forwarding misinformation to others. A user activity report highlighting the misinformation might lead to useful prompts and guidance to relevant educational content.

## SITUATIONAL AWARENESS

It may be beneficial to exchange threat intelligence information that aids situational awareness and helps link events with other domains. Post-incident review of user settings could also fall under this functionality group.

## CONCLUSIONS AND FUTURE WORK

The considerable concern about disinformation, the importance of democratic values and the degree of uncertainty expressed by users in their ability to identify disinformation correctly suggests the need to strengthen protection at endpoints and indicates that users may be willing to adopt the proposed functionality. The technological gap or privacy concerns may prove to be barriers for some people. Generative AI can prove particularly helpful in bridging technological gaps in user support, as would the use of optimal default profile settings. Raising awareness of privacy-enhancing technologies could alleviate fears and assure privacy protection.

Privacy-enhancing technologies such as differential privacy and federated learning could enable the utility of relevant data while assuring their privacy in accordance with data protection principles. This is particularly important for supporting detection and response, situational awareness or user profiling, where the privacy requirements would be higher. As the focus is on examining content rather than user behaviour, it could be argued that the privacy requirements of support, education and threat space reduction functionality would be relatively lower. In any case, the privacy requirements of any endpoint functionality must be determined and justified before seeking user consent.

The proposed endpoint functionality aims to complement existing defences and social media controls by democratizing protection. It seeks to empower users with the right and responsibility to control their own information space, irrespective of their social media applications, encouraging transparency. It aims to bridge the technological gap between humans and disinformation controls, maximize support, reduce the likelihood of human error, and promote secure behaviour as the norm. It also strives to offer freedom of choice to individuals in cases where centralized controls could risk eroding democratic values and human rights. A conceptual architecture, requirements analysis, use cases and proof of concept functionality could extend this work in future to illustrate its key points. ■

**MARIA PAPADAKI**

Dr Maria Papadaki is an associate professor in Cyber Security at the University of Derby, UK. Her research interests focus on incident response, threat intelligence, maritime cybersecurity, and human-centred security. Her research outputs include more than 70 international peer-reviewed publications in this area. The views contained in this article are the author's alone and do not represent the views of the University of Derby.


## ENDNOTES


[1] European Commission, 'Flash Eurobarometer 536 Report: Public awareness and trust in European statistics', February 2024, https://europa.eu/eurobarometer/surveys/detail/2955.

[2] European Parliament, 'Media & News Survey 2023', November 2023, https://europa.eu/eurobarometer/surveys/detail/3153.

[3] OFCOM, 'News consumption in the UK: 2023, Research findings', July 2023, https://www.ofcom.org.uk/media-use-and-attitudes/attitudes-to-news/news-consumption/.

[4] Idem.

[5] Urbano Reviglio and Claudio Agosti, 'Thinking Outside the Black-Box: The Case for "Algorithmic Sovereignty" in Social Media', Social Media + Society Volume 6 Issue 2 (April 2020), https://doi.org/10.1177/2056305120915613.

[6] Lisa O'Carroll, 'Disinformation networks "flooded" X before EU elections, report says', July 2024, https://www.theguardian.com/world/article/2024/jul/12/disinformation-networks-social-media-x-france-germany-italy-eu-elections.

[7] World Economic Forum, 'The Global Risks Report 2023: 18th Edition Insight Report', January 2023, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

[8] European Parliament, 'Eurobarometer: Parlemeter 2022', January 2023, European Commission, 'Flash Eurobarometer 536 Report: Public awareness and trust in European statistics', February 2024, https://europa.eu/eurobarometer/surveys/detail/2955.

[9] Seumas Miller, 'Cognitive warfare: An ethical analysis', Ethics and Information Technology Volume 25, Issue 46 (September 2023), https://doi.org/10.1007/s10676-023-09717-7.

[10] Nicolas Hénin, 'FIMI: Towards a European redefinition of Foreign Interference', EU Disinfo Lab, April 2023, https://www.disinfo.eu/publications/fimi-towards-a-european-redefinition-of-foreign-interference/.

[11] Erika Magonara and Apostolos Malatras, 'Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape', ENISA, December 2022, https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape/.

[12] Jakub Kalenský and Roman Osadchuk, 'How Ukraine fights Russian disinformation: Beehive vs mammoth', Hybrid CoE Research Report 11, January 2024.

[13] King's College London and Ipsos, 'Emerging tensions? How younger generations are dividing on masculinity and gender equality', February 2024, https://www.kcl.ac.uk/policy-institute/assets/emerging-tensions.pdf.

[14] Marianna Spring, '"It stains your brain": How social media algorithms show violence to boys', BBC Panorama, September 2024, https://www.bbc.co.uk/news/articles/c4gdqzxypdzo.

[15] NPCC, 'Violence Against Women and Girls (VAWG): National Policing Statement 2024', July 2024, https://cdn.prgloo.com/media/5fc31202dd7e411ba40d29fdca7836fd.pdf.

[16] Mark Easton, 'Protests reveal deep-rooted anger, but UK is not at boiling point', August 2024, https://www.bbc.co.uk/news/articles/czx66dkx3wlo.

[17] Marianna Spring, 'Did social media fan the flames of riot in Southport?', July 2024, https://www.bbc.co.uk/news/articles/cd1e8d7llg9o.

[18] European External Action Service (EEAS), '2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence', January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[19] World Economic Forum, 'The Global Risks Report 2023: 18th Edition Insight Report', January 2023, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

[20] European External Action Service (EEAS), '2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence', January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[21] Luke Hurst, 'How a fake image of a Pentagon explosion shared on Twitter caused a real dip on Wall Street', Euronews, May 2023, https://www.euronews.com/next/2023/05/23/fake-news-about-an-explosion-at-the-pentagon-spreads-on-verified-accounts-on-twitter.

[22] Shahbaz, Funk, and Vesteinsson, 'The Repressive Power of Artificial Intelligence', in Freedom on the Net 2023, Shahbaz, Funk, Vesteinsson, Brody, Baker, Grothe, Barak, Masinsin, Modi, and Sutterlin, eds (Freedom House, 2023), freedomonthenet.org.

[23] Idem.

[24] World Economic Forum, 'The Global Risks Report 2023: 18th Edition Insight Report', January 2023, https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf.

[25] European Commission, 'Flash Eurobarometer 464: Fake news and disinformation online', April 2018, https://europa.eu/eurobarometer/surveys/detail/2183.

[26] European External Action Service (EEAS), '2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence', January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[27] European External Action Service (EEAS), '1st EEAS Report on Foreign Information Manipulation and Interference Threats towards a framework for networked defence', February 2023, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf.

[28] European External Action Service (EEAS), '2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence', January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[29] Rakoen Maertens, Friedrich M. Götz, Hudson F. Golino, Jon Roozenbeek, Claudia R. Schneider, Yara Kyrychenko, John R. Kerr, Stefan Stieger, William P. McClanahan, Karly Drabot, James He, and Sander van der Linden, 2024, 'The Misinformation Susceptibility Test (MIST): A psychometrically validated measure of news veracity discernment', Behaviour Research Methods Volume 56, 1863–1899 (March 2024), https://doi.org/10.3758/s13428-023-02124-2.

[30] Linley Sanders, 'How well can Americans distinguish real news headlines from fake ones?', June 2023, https://today.yougov.com/politics/articles/45855-americans-distinguish-real-fake-news-headline-poll.

[31] European Parliament, 'Media & News Survey 2022', July 2022, https://europa.eu/eurobarometer/surveys/detail/2832.

[32] OFCOM, 'The genuine article? One in three internet users fail to question misinformation', March 2023, https://www.ofcom.org.uk/media-use-and-attitudes/attitudes-to-news/one-in-three-internet-users-fail-to-question-misinformation/.

[33] Verizon, '2024 Data Breach Investigations Report', May 2024, https://www.verizon.com/business/resources/reports/dbir/.

[34] Lance Spitzner, 'Why a Phishing Click Rate of 0% is Bad', November 2017, https://www.sans.org/blog/why-a-phishing-click-rate-of-0-is-bad/.

[35] Shreya Ghosh and Mitra Prasenjit, 2023.'"Review of How Early Can We Detect? Detecting Misinformation on Social Media Using User Profiling and Network Characteristics', in Lecture Notes in Computer Science, Gianmarco De Francisci Morales, Claudia Perlich, Natali Ruchansky, Nicolas Kourtellis, Elena Baralis, and Francesco Bonchi, eds, Vol. 14174, Springer. https://doi.org/10.1007/978-3-031-43427-3_11.

[36] Idem.

[37] Frederico Monti, Fabrizio Frasca, Davide Eynard, Damon Mannion, and Michael M. Bronstein, 'Review of Fake News Detection on Social Media Using Geometric Deep Learning', in: Representation Learning on Graphs and Manifolds Workshop, ICLR 2019, May 2019, Ernest N. Morial Convention Center, New Orleans, USA, https://rlgm.github.io/papers/34.pdf.

[38] Microsoft, 2023, 'Microsoft Digital Defense Report: Building and improving cyber resilience', October 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[39] Md Shohel Rana, Mohammad Nur Nobi, Beddhu Murali, and Andrew H. Sung, 'Deepfake Detection: A Systematic Literature Review', in IEEE Access, Volume 10, 25494–25513, 2022, doi: 10.1109/ACCESS.2022.3154404.

[40] Yingtong Dou, Kai Shu, Congying Xia, Philip S. Yu, and Lichao Sun, 2021, July, User preference-aware fake news detection, in Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval (2051–2055).

[41] 'DISARM Framework Explorer', DISARM Frameworks, last modified November 2023, https://disarmframework.herokuapp.com/.

[42] EU Disinfo Lab, 'Tools to monitor disinformation', 2024, https://www.disinfo.eu/resources/tools-to-monitor-disinformation/.

[43] European External Action Service (EEAS), '2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A framework for networked defence', January 2024, https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf.

[44] EU Disinfo Lab, 'Tools to monitor disinformation', 2024, https://www.disinfo.eu/resources/tools-to-monitor-disinformation/.

# THEN WE WILL FIGHT IN THE SHADE

// Matthias Wasinger

**ABSTRACT:** The recognition of existential threats such as cognitive warfare is crucial to avoid defeat. Western societies must address such threats by leveraging their militaries' adaptability. Relying solely on the military poses risks, however, necessitating a comprehensive approach to national security. Coordination among all the instruments of power under democratic control is essential for effective outcomes. Western militaries should focus on deterrence and support political decision making. Cognitive warfare targeting civilians requires continuous societal education and enhanced governmental information capabilities. While international law addresses various challenges, there may not be a legal solution for those arising from cognitive warfare. In the face of modern threats Europe may need to defend its values through comprehensive, coordinated and synchronized means.

**BOTTOM-LINE UPFRONT:** Wars are often waged with instruments other than military force. Nevertheless, the military can support the response to a threat. Besides hard power, militaries can provide political leadership with valuable advice, procedures and techniques to enable them to counter existential threats.

**PROBLEM STATEMENT:** How can the military instrument of power be used to counter cognitive warfare?

**SO WHAT?** The modern state has more than just one instrument of power. Coordinated and synchronized, such instruments can achieve the most effective and efficient outcomes in concertation. The military's role in this orchestra should be twofold. It must ensure credible deterrence while providing valuable processes, procedures and techniques.

## UNFAIR GAME; TWO APPROACHES

According to Herodotus, when threatened by the Persians with such a multitude of arrows that they obscured the sun during the Battle of Thermopylae in 480 BCE, the Spartan warrior Dienekes responded, "Then we will fight in the shade".[1] In subsequent centuries several statesmen and philosophers have reattributed and reinterpreted this quotation. Its original meaning has evolved. The original statement underlined the paradoxically advantageous effect of fighting in the shade instead of under the blazing sun.[2] Another possible interpretation was added over the centuries, however: forbearance in clear sight of an overwhelming threat.[3] Confronted by an existential threat, ancient Greece, European culture's cradle, set the scene for winning a war by seeking an advantage in inferiority or defiant resistance.

More than two thousand years later Europe again faces an existential threat. Russia's recent invasion of Ukraine is not a mere inter-state conflict at the continent's eastern edges. It is part of a campaign that seeks to eradicate the Western way of life, the recognized international legal framework, European values and supranational cohesion.[4] To this end, Russia and its partners have long waged a hybrid war against Europe. Unlike the Persian Wars, the weapons are no longer arrows. Disinformation campaigns, information warfare and cognitive warfare endanger social cohesion, transnational solidarity and public support for resistance to the external threat.[5] These means clearly fall below the threshold of armed conflict yet still challenge Western societies.[6] Once the threat is recognized and acknowledged, however, Europe may decide how to fight back by finding the advantage in turmoil or defiant forbearance.

## NO RESPONSE WITHOUT RECOGNITION

The cornerstone of any response to a threat is its official political recognition. As plain as this sounds, Europe especially still lacks situational awareness. Russia's military intrusions in Georgia in 2008 and Ukraine in 2014 were not followed by international condemnation or isolation.[7] On the contrary, a policy of appeasement and the deepening of economic dependence, especially on fossil energy, led to public ignorance of a painful fact: Russia's assertiveness was no longer limited to the diplomatic domain. Even the Russian government's blatant – and unfortunately successful – attempts to "hire" former high-ranking European politicians, including former German chancellor Gerhard Schröder and former French prime minister François Fillon, to gain an even deeper foothold in European political decision making were not taken seriously.[8] Even Russia's most recent invasion of Ukraine is still not recognized for what it is: a frontal attack on international law and order and European values.

The ongoing attritional warfare in Ukraine is just the most obvious symptom of Russia's aggression. Beneath this most cruel and visible campaign Russia and its partners are waging a more clandestine war against the West. It is a war for dominance in the information domain, a battle for superiority in attributing and interpreting information.[9] The aim is to shape how societies think about and influence the understanding of past, ongoing and future events and to diminish – if not annihilate – Western societies' trust and belief in values and their willingness to stand up for them.[10]

Although Western societies' support for Ukraine is remarkable and has undoubtedly enabled it to resist Russian aggression so far,[11] one might question whether the problem's entirety is recognized as a threat not

only to a country on Europe's eastern edge but also as an attack on democratic concepts. Meanwhile, funds continue to flow to Ukraine, and weapon systems and ammunition are slowly but steadily being delivered to the East. Most European nations still lag in their energy independence, autonomous military deterrence and social resilience targets.[12] It seems the superstition prevails that the current friction will be over one day, followed by a return to a new normal, with mutual trust, recognition of international law and good order.

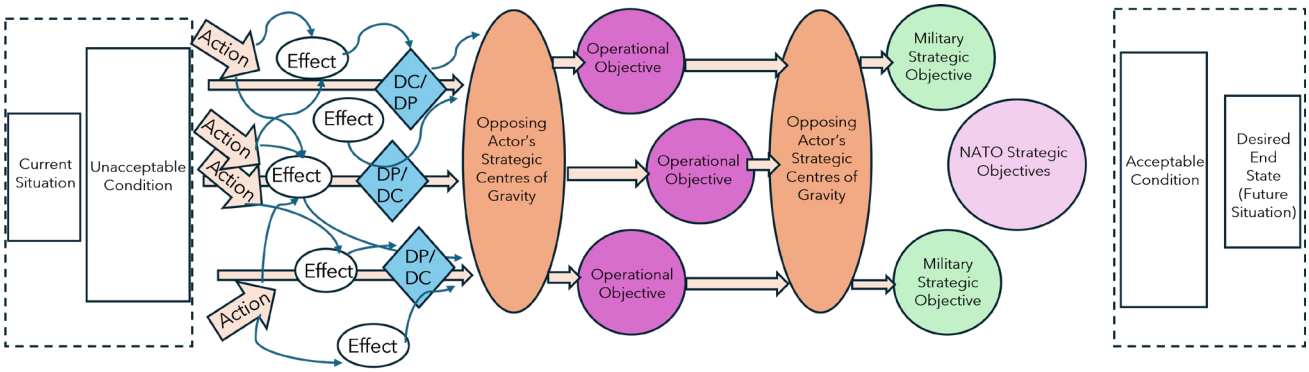
Apparently, Russia's openly belligerent diplomatic, economic and even military threat posture has not (yet) crossed the threshold to be recognized for what it is – an existential threat.[13] Political statements outline the obvious. War does not begin with troop movements, economic blackmail, nuclear brinkmanship, cyberattacks, targeted killings, espionage and obvious human rights violations. It does not begin with strategic bombers and tanks crossing internationally recognized borders.[14] [15] Both the People's Republic of China's "Unrestricted Warfare" and Russia's "Active Measures" clearly illustrate this.[16] Even if Western leaders wish to apply the legally institutionalized definition of war, these endeavours are in vain as long as one side decides no longer to acknowledge them. Clausewitz famously compared war with a wrestling match in which one side tried to compel the other to submit.[17] Cognitive warfare does exactly that. Peace needs the commitment of two sides; war only one. Wars start when political leaders recognize and declare (decide) that a war has started. As inconvenient as this decision appears, even with obvious belligerent deeds, it is more difficult to recognize clandestine acts below the threshold of conventional warfare as acts of war. Yet philosophy is the precursor of reality and the historical example: ignoring the multitude of incoming arrows may avoid a fight but not their deadly effect. The arrows are real, and they are aimed at the West.

Antagonist powers' attacks occur in the cognitive dimension. Cognitive warfare includes activities synchronized with other instruments of power to affect attitudes and behaviours by influencing, protecting or disrupting individual, group or population-level cognition to gain an advantage over an adversary. Whole-of-society manipulation has become a new norm designed to modify perceptions of reality, with the shaping of human cognition a critical warfare realm.[18] Given this definition, how can the military instrument of power counter or meaningfully support endeavours to counter such warfare? Defiant military forbearance or creativity in ambiguity? Waiting for a military escalation or comprehensive counteraction?

## IF ALL YOU HAVE IS A HAMMER, EVERYTHING LOOKS LIKE A NAIL

The term cognitive warfare lends itself to an attribution to the military instrument of power. Ideally, states run a military to wage war or to respond to existential threats. Consequently, if cognitive warfare existentially threatens a state by attacking its social cohesion, delegitimizing its political leadership and even interfering in every democracy's highest good – elections – military means may be used to counter the threat. Cognitive warfare integrates cyber, information, psychological and social engineering capabilities,[19] all of which are available in the military.

To solve a problem, most Western militaries follow distinct planning steps. Political objectives are translated to military objectives. These objectives contribute to achieving a defined desired end state. (Decisive) conditions and effects, created by military and complementary non-military actions, define a roadmap for getting from an unacceptable to an acceptable condition.[20]




Source: COPD[21]

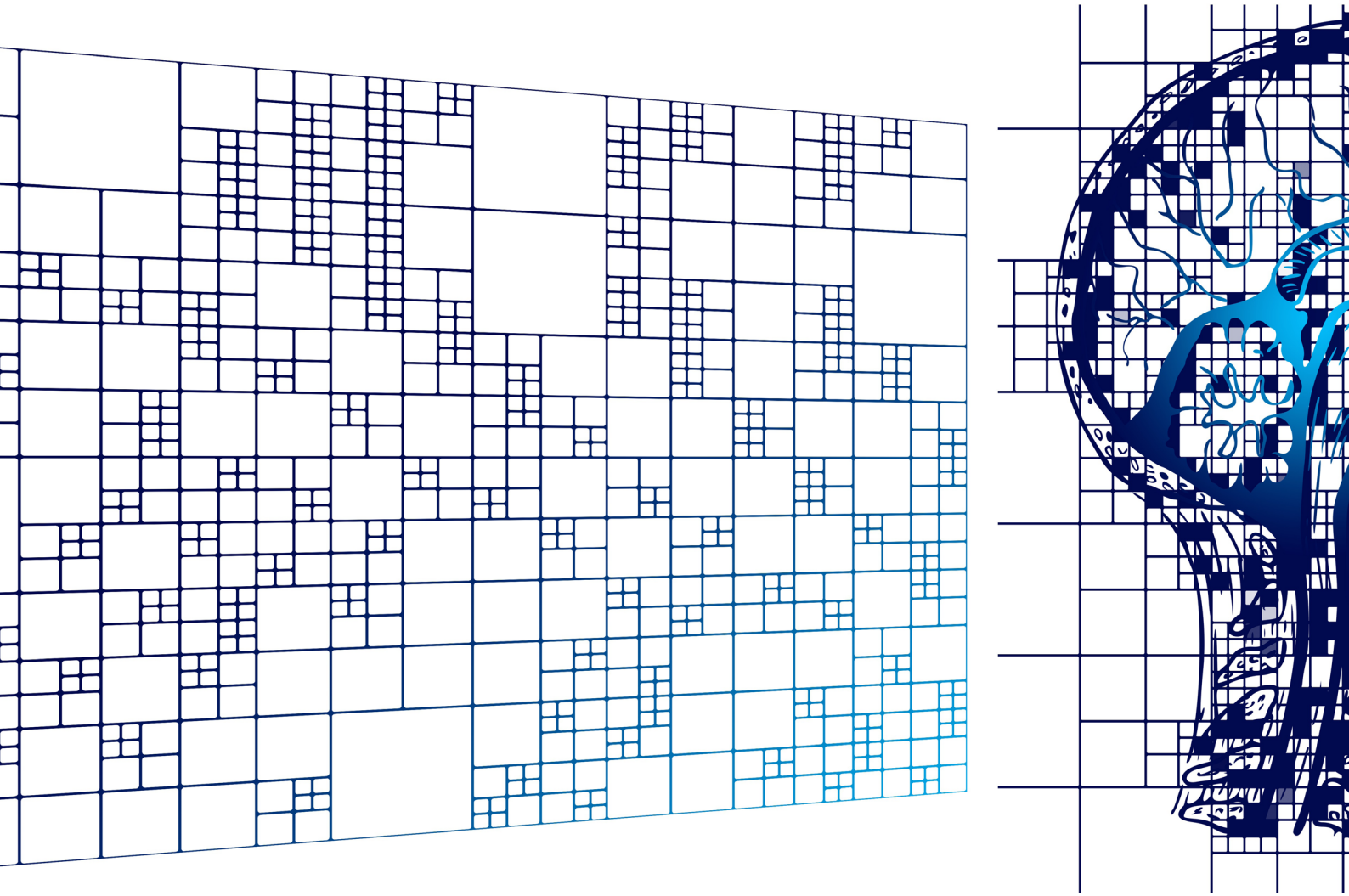
Whereas the collaborative planning process involves several levels of command, including institutional creativity and expertise, and the actual deeds on the ground, actions are (mainly) defined by those commands fighting in warfighting domains.[22] Although there is no commonly agreed definition of a warfighting domain, it can be defined as organizational constructs comprising an area of responsibility with a unique operational environment requiring distinct tactics, equipment and structure.[23] Likewise, NATO defines an operational domain as "a specified sphere of capabilities and activities that can be applied within an engagement space".[24]

Undoubtedly, cognitive warfare takes place in a (functional rather than geographical) area of responsibility within a unique operational environment, namely the human mind. Equipment and structures are derived from tasks and tactics. Yet these necessary tactics go beyond the doctrinal and indeed legal limitations of Western militaries. Western military doctrines explicitly exclude their populations from influence operations.[25] Besides, military efforts to shape how nations' populations think are clearly beyond Western societies' legal frameworks. Apparently, there is no cognitive warfighting domain;[26] and even if there were, Western militaries would be prohibited from operating in it against their own populations.

Moreover, for such an operational environment, military terminology appears too absolute, too Mahanian. Terms such as supremacy and superiority imply a kind of unchallenged dominance in respective dimensions. In an age of digitalization and connectivity information freely circulates online in accordance with European values. In this context cyberspace is both a means of transmission and a warfighting domain for disinformation, as well as information and cognitive warfare. Cyberspace has essentially facilitated the creation of the vitreous human and – potentially – transparent society. Digitalization and the everyday use of cyberspace have turned this artificial domain into a place of actual consequence, a diplomatic tool, an economic factor, a military effector and a social space satisfying the human need for social connectivity, for example. Cyberspace has contributed to the democritization of information while allowing malign actors to influence target audiences, set and dominate narratives, and exploit information.[27] No absolute supremacy in the cognitive dimension uses mainly democratized cyberspace.

The ongoing war in Ukraine has emphasized the dominance of a more Corbettian approach, meaning the necessity to achieve conditions that are good enough to make the best use of a certain (functional) area for a defined period.[28] This in turn seems achievable in both practical and legal terms, as the aim is neither social indoctrination nor permanent cognitive alignment. It remains questionable, however, whether the military is the most suitable instrument of power to do this.

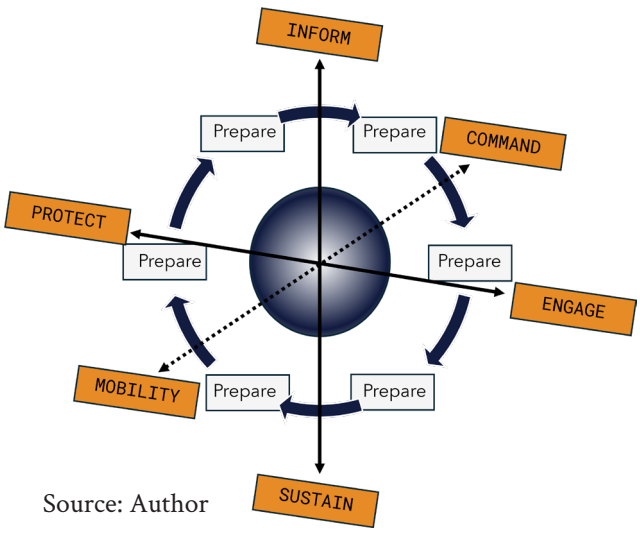
The military instrument of power is a nation's executive approach to external threats. This fact clearly distinguishes it from internally oriented police forces.[29] Tasking the military with either waging or countering cognitive warfare seems an obvious but futile choice. Although appropriate planning mechanisms are in place, neither a military's characteristics nor its democratically legitimized framework and organizational culture as a nation's existential guardian make it the right tool for the task. Cognitive warfighting brigades will not solve the problem. They would fight in the dark in defiant forbearance, restricted, ill equipped, inappropriately trained and ultimately without achieving the desired effect.



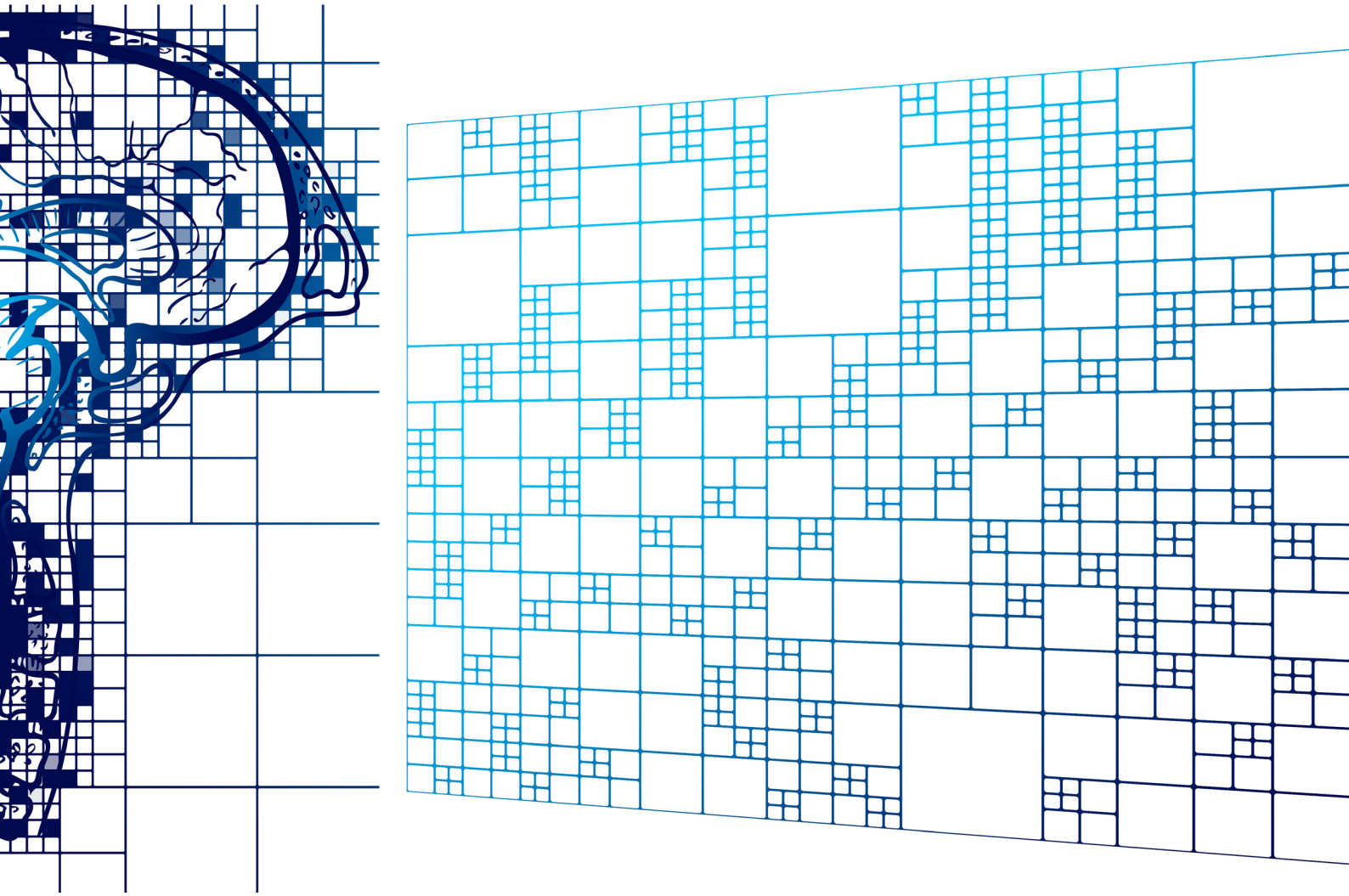
## ADVANTAGE IN AMBIGUITY

Cognitive warfare must be waged in synchronicity with other instruments of power to affect attitudes and behaviours. Military warfighting domains and dimensions such as cyberspace, the electromagnetic spectrum and the information realm are mere facets of a comprehensive concept. As such, the threats are not only a technical hack. They holistically harm our societies. They undermine democracies by diminishing both people's trust in politics and their willingness to defend our way of life. They challenge the legal and ethical framework by exploiting Western adherence to the rule of law and liberalism. (More or less) reasonable doubts, alternative truths and plausible deniability target human psychology in the information age. All these endeavours lead to geopolitical shifts that marginalize Europe's role on the world stage.[30] Holistic challenges call for comprehensive answers! The problem's solution therefore cannot be found in a single instrument of (hard) power.

Countering cognitive warfare and effectively responding to it if necessary (and appreciating its relevance for military planning and operations' execution) is mainly about preparation. All military capability areas – command, engage/operate, sustain, mobility/project, protect and inform – are based on proper preparation. Countering cognitive warfare in the "current" inevitably leads to a struggle for narrative dominance, the "absolute truth" and superior interpretation.[31] Unfortunately, Western societies have had to learn that "factual truth" as such does not matter. Once a narrative dominates the information realm, people's way of thinking is already shaped. Examples of this phenomenon range from the well-known (but non-existent) promise to Gorbachev concerning the inclusion of former Warsaw Pact states in NATO to Vladimir Putin's historical (but irrelevant and sometimes even absurd) claims on Ukraine.[32] [33] [34] Subjective truth – and only this matters to the individual – lies in people's beliefs. "Truth" lies in one's perception, and war happens when politicians say there is a war, not when tanks cross a border.




Source: Author



Russia has been at war with the West since Vladimir Putin stated this publicly on several occasions, among others during the 2008 Munich Security Conference.[35] It is a war that is still not actively waged with military means outside Ukraine. This should in turn mean that the West is at war too. Political leaders must face this inconvenience and accept it as fact. It is not a war the West chose to wage. It is a war that was imposed on the West, no matter how blatantly Vladimir Putin spins the facts. Western societies should therefore ensure both military deterrence and social resilience in all domains, dimensions and realms, and exploit strategic ambiguity. A society that is well informed about a state of war (especially one that is not waged by military means) is more willing to develop, support and contribute to deterrence and resilience.[36]

Indeed, a huge amount of work remains to be done in fields such as education (e.g. intellectual national defence, national security and defence policy, European values), governmental, semi-governmental and civil economy (strategic autonomy, national stockpiling), society (social cohesion, plurality, inclusivity and diversity management), and information technology (the value and curse of social media, digital literacy). Nevertheless, there is indeed a need for a military contribution. Militaries have developed processes and procedures throughout history that work in the worst imaginable circumstances and still deliver viable solutions.

Democracies have deficiencies in defining strategic objectives.[37] The military is capable of providing procedures to develop and frame achievable objectives.[38] A nation's sensors are so numerous, and the lines of communication so vast and complex, that achieving situational awareness is demanding. However, militaries have developed concepts to deal with complexity and complications.[39] Relations and connections between and within societies are multi-layered and shaped, among other factors, by history, culture and religion, so it is challenging to obtain and maintain a comprehensive understanding of social interaction.

Nevertheless, militaries have developed techniques to create, within means and capabilities, a comprehensive understanding of relevant actors, their interests, strengths, weaknesses and interconnections, even for out-of-area operations.[40] Through intrinsic need militaries have the ability to frame problems and define efficient approaches, structures, organizations and ultimately viable courses of action. Militaries possess the tools required to define effects and target audiences, assess risks and appropriate mitigating measures, and measure progress while advancing from an unacceptable to an acceptable status. They have all these tools and can provide them to decision makers, even without being the leading instrument of power.

This is not, of course, a call to reinvigorate militarism. Moreover, when emphasizing the need for political supremacy over the military instrument of power, Carl von Clausewitz explicitly mentioned the sovereign's need to appreciate the (military) experts' best advice.[41] When Clausewitz wrote On War, he did so from the perspective of a sovereign who controlled only one instrument of power, the military. We can assume that had they existed, he would have extended his theory to all other instruments of power.

Although a war may be waged with instruments other than the military, the military can offer support in response to non-kinetic/below-threshold threats such as cognitive threats. In doing so, it is indeed vital not to become a militaristic society. Besides military hard power, a crucial element of deterrence is maintaining and even expanding soft power – namely, European values, liberty and diversity.[42] There is nothing antagonist powers fear more than our open liberal democratic system.[43] Liberal democracy disqualifies the foundation of their power apparatus and ultimately delegitimizes their governance. Fighting in the shade allows the exploitation of strategic ambiguity. Necessary preparatory measures can be taken in the shade instead of under the blazing sun.

## FIGHTING IN THE SHADE

To solve a problem, one must recognize that there is one in the first place. Ignoring it will inevitably lead to defeat. Once Western societies take that crucial step, political leaders must decide how to address these multidimensional existential threats: by finding the advantage in turmoil or defiant forbearance. Attributing the preparation for any kind of warfare to the nation's warfighting instrument appears an obvious solution. Leaders should be aware of military adaptability and inherent obedience. This instrument of power will certainly take up the task and live up to it within its means and capabilities. Yet however adaptable we are, there is a risk that the hammer will treat the problem like a nail, especially given the (definitely required) legal restrictions. In forbearance the military would reactively fight with both hands tied behind its back in a dimension that asked for more comprehensiveness.

Fortunately, the modern state has more than just one instrument of power. Coordinated and synchronized, under the control of legitimized democratic leaders they can achieve the most effective and efficient outcomes in concertation. The military's role in this orchestra should be twofold. On the one hand it must deliver its raison d'être – namely, deterrence. On the other it can provide valuable processes, procedures and techniques to both the political leadership itself and other instruments of power.

Ultimately, one should bear in mind that cognitive warfare targets mainly civilians, the democratic sovereign. This is not a new phenomenon. About a hundred years ago, when elaborating on air power and military deep operations, Giulio Douhet wrote, "There will be no distinction any longer between soldiers and civilians. The defence on land and sea will no longer serve to protect the country behind them; nor can victory on land or sea protect the people…"[44] Humankind has found a solution to the problem in international law. This does not mean there will be a legal solution to the challenges imposed on the West by cognitive warfare. It is more likely that it will be an impetus to further educate societies or develop governmental information skills. One way or another it seems inevitable that Europe will again have to defend its existence and values by fighting in the shade. ■


**MATTHIAS WASINGER**

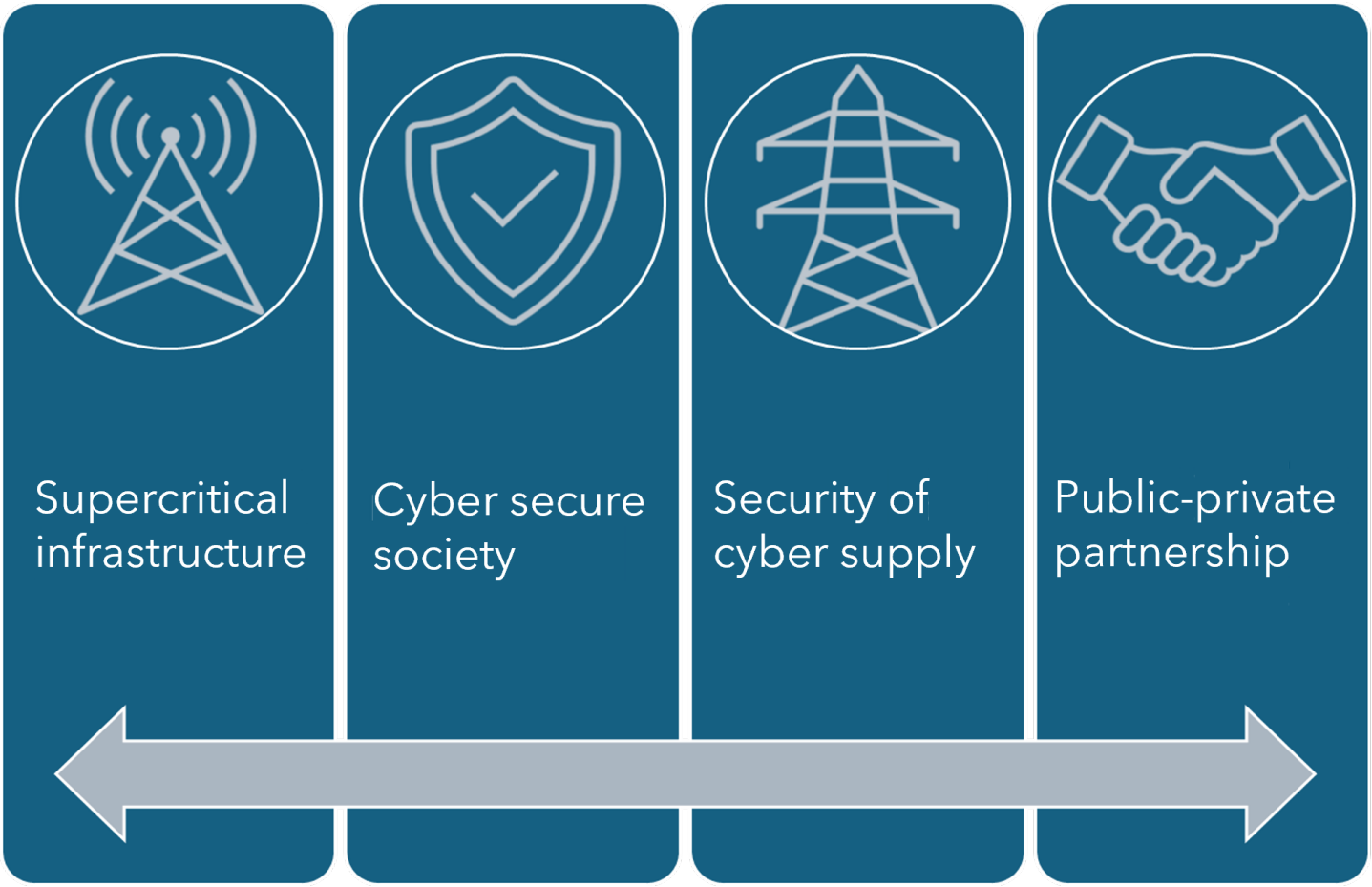
Matthias Wasinger is a colonel (GS) in the Austrian Armed Forces. He holds a Magister in Military Leadership (Theresan Military Academy), a master's degree in Operational Studies (US Army Command and General Staff College), and a PhD in Interdisciplinary Studies (University of Vienna). He has served both internationally and nationally at all levels of command. He is also the founder and editor-in-chief of The Defence Horizon Journal. He has served at the International Staff/NATO Headquarters in Brussels since 2020. The views expressed in this paper are the author's alone.

## ENDNOTES


[1] Herodotus, The Histories Book 7: Polymnia (Start Publishing LLC, 2015).
[2] Plutarch, Apophthegmata Laconica (Loeb Classical Library edition, Vol III, 1931).
[3] Valerius Maximus, Factorum et dictorum memorabilium, liber III.
[4] Peter Dickinson, 'Putin's Poisonous Anti-Western Ideology Relies Heavily on Projection', Atlantic Council, 3 July, 2022, accessed 7 March, 2024, https://www.atlanticcouncil.org/blogs/ukrainealert/putins-poisonous-anti-western-ideology-relies-heavily-on-projection/.
[5] Matthias Wasinger, 'The Highest Form of Freedom and the West's Best Weapons to Counter Cognitive Warfare', TDHJ.org, accessed 21 May, 2024, https://tdhj.org/blog/post/freedom-counter-cognitive-warfare/.
[6] Robert Seely, 'Defining Contemporary Russian Warfare', The RUSI Journal Volume 162, Issue 1 (2017): https://doi.org/10.1080/03071847.2017.1301634.
[7] Akaki Dvali, 'From Appeasement to Accountability – The West's New Approach Can Save Georgia from Putin', Newsweek, 19 March, 2024, accessed 11 May, 2024, https://www.newsweek.com/appeasement-accountability-wests-new-approach-can-save-georgia-putin-opinion-1880600.
[8] Hodun, Milosz and Cappelletti, Francesco, eds, Putin's Europe: Russia's Influence in European Democracy (ELF, 2023), 176–177.
[9] Geoffrey Roberts, '"Now or Never": The Immediate Origins of Putin's Preventative War on Ukraine', Journal of Military and Strategic Studies Volume 22, Issue 2 (2022).
[10] Ian Garner, 'The West Is Still Oblivious to Russia's Information War', Foreign Policy, 2024, accessed 11 May, 2024, https://foreignpolicy.com/2024/03/09/russia-putin-disinformation-propaganda-hybrid-war/.
[11] Congressional Research Service, Russia's War Against Ukraine: European Union Responses and U.S.-EU Relations (2024), https://crsreports.congress.gov/product/pdf/IN/IN11897.
[12] Council of the European Union, '"If We Want Peace, We Must Prepare for War"', news release, 19 March, 2024, accessed 11 May, 2024, https://www.consilium.europa.eu/en/press/press-releases/2024/03/19/if-we-want-peace-we-must-prepare-for-war/.
[13] Michael P. o. Liechtenstein, 'Is a Broader European War Imminent?', GIS, 2024, accessed 11 May, 2024, https://www.gisreportsonline.com/r/is-european-war-imminent/.
[14] Rosa Brooks, 'Can There Be War Without Soldiers?', Foreign Policy, 2016, accessed 11 May, 2024, https://foreignpolicy.com/2016/03/15/can-there-be-war-without-soldiers-weapons-cyberwarfare/.
[15] Seth G. Jones, Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare (New York, NY: W. W. Norton & Company, 2021), 73–76.
[16] Seth G. Jones, Three Dangerous Men: Russia, China, Iran, and the Rise of Irregular Warfare (New York, NY: W. W. Norton & Company, 2021).
[17] Carl von Clausewitz, On War, ed. Michael Howard Princeton, NJ [u.a.]: Princeton Univ. Press, 1989, 75.
[18] Allied Command Transformation, Cognitive Warfare (2024), accessed 10 February, 2024, https://www.act.nato.int/activities/cognitive-warfare/.
[19] Idem.
[20] Allied Command Transformation, Comprehensive Operations Planning Directive: COPD INTERIM V2.0, 4–32 – 4–110.
[21] Ibid., 4–53.
[22] Ibid., 4–32 – 4–110.
[23] Everett C. Dolman, 'Space Is a Warfighting Domain', ÆTHER: A JOURNAL OF STRATEGY & AIRPOWER 1, Volume 1 (2022): 84, accessed 10 March, 2024, https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-1_Issue-1/11-Dolman.pdf.
[24] Allied Joint Publication-01, AJP-01 (NATO), no. 01, LEX-06.
[25] AJP-3.10, Allied Joint Doctrine for Information Operations (NATO), no. 3.10, 1–2 – 1–10.
[26] Patrick Hofstetter and Flurin Jossen, 'There Is No Need for a Cognitive Domain', TDHJ.org, 2 November, 2023, accessed 13 May 2024, https://tdhj.org/blog/post/no-need-cognitive-domain/.
[27] Matthias Wasinger, 'The Highest Form of Freedom and the West's Best Weapons to Counter Cognitive Warfare', TDHJ.org, accessed 21 May, 2024, https://tdhj.org/blog/post/freedom-counter-cognitive-warfare/.
[28] Julian S. Corbett, Some Principles of Maritime Strategy: A Theory of War on the High Seas; Naval Warfare and the Command of Fleets (Adansonia Press, 2018), 71–141.
[29] Matthias Wasinger, 'Vom Wesen und Wert des Militärischen: Interdisziplinäre Reflexion zum Alleinstellungsmerkmal des Militärischen zwischen Anspruch und Wirklichkeit' (Dissertation, Faculty of Law, 2017), 54–55.
[30] Matthias Wasinger, 'The Highest Form of Freedom and the West's Best Weapons to Counter Cognitive Warfare', TDHJ.org, accessed 21 May, 2024, https://tdhj.org/blog/post/freedom-counter-cognitive-warfare/.
[31] See for example: Government of Canada, 'Countering Disinformation with Facts – Russian Invasion of Ukraine', Government of Canada, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng.
[32] Jeff Neal, '"There Was No Promise Not to Enlarge NATO" – Harvard Law School', Harvard Law School, accessed 14 May, 2024, https://hls.harvard.edu/today/there-was-no-promise-not-to-enlarge-nato/.
[33] NATO, 'NATO – Official Text: Founding Act on Mutual Relations, Cooperation and Security Between NATO and the Russian Federation Signed in Paris, France, 27 May 1997', accessed 13 May 2024, https://www.nato.int/cps/su/natohq/official_texts_25468.htm.
[34] Government of Canada, 'Countering Disinformation with Facts – Russian Invasion of Ukraine', Government of Canada, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-fact-fait.aspx?lang=eng.
[35] Nick Fishwick, 'Putin Has Declared War on the West. It's Time to Take the Fight to Russia', The Cipher Brief, 19 February, 2024, accessed 9 May, 2024, https://www.thecipherbrief.com/column_article/putin-has-declared-war-on-the-west-its-time-to-take-the-fight-to-russia.
[36] Michal Onderco, Wolfgang Wagner, and Alexander Sorg, WHO ARE WILLING to FIGHT for THEIR COUNTRY, and WHY? (2024), accessed 7 May, 2024, https://spectator.clingendael.org/en/publication/who-are-willing-fight-their-country-and-why.
[37] Donald J. Stoker, Why America Loses Wars: Limited War and US Strategy from the Korean War to the Present, Revised and updated [edition] (Cambridge: Cambridge University Press, 2022), 53–60.
[38] Allied Command Transformation, Comprehensive Operations Planning Directive: COPD INTERIM V2.0, 3–19 – 3–36.
[39] NATO Science and Technology Organization, 'Visualisation and the Common Operational Picture', accessed 13 May, 2024.
[40] Allied Command Transformation, Comprehensive Operations Planning Directive: COPD INTERIM V2.0, 4–13 – 4–48.
[41] Carl von Clausewitz, On War, ed. Michael Howard, (Princeton, NJ [u.a.]: Princeton Univ. Press, 1989), 608–609.
[42] Robert Service, The Penguin History of Modern Russia: From Tsarism to the Twenty-First Century, 4th ed. (London, UK: Penguin, 2021), 571–591.
[43] Timothy Frye, Weak Strongman: The Limits of Power in Putin's Russia (Princeton and Oxford: Princeton University Press, 2021), 12–14.
[44] Giulio Douhet, The Command of the Air, USAF warrior studies Washington, D.C.: Air Force History and Museums Program, 1942, 10.


# CYBERWATCH FINLAND – CHALLENGES AND RESILIENCE OF MODERN DIGITAL SOCIETY

# SUMMARY OF THE WHITE PAPER




Picture 1. Four pillars of crisis-resilient society

Digitalisation and the changing international operating environment challenge Western societies, raising new challenges and needs for development. Russia's war of aggression against Ukraine and its other cyber activity has widely opened eyes to these threats as well. In addition, increasing cybersecurity regulation will increase organisations' security responsibilities in this area. The most significant news this autumn is the entry into force of the NIS2 Directive in Europe. Several significant cyber reports and strategies are also being prepared during 2024.

The cyber environment is in the midst of constant change. Cyberwatch Finland, a strategic cybersecurity consultancy house, actively monitors and produces cyber situational awareness. We also want to share this information more widely. In order to develop the comprehensive security of society, information siloes should be avoided and good practices should be spread widely. The cyber industry also needs new ideas, lessons learned from the past events, as well as constructive discussion on the development of cybersecurity.

Against this background, Cyberwatch Finland published a white paper on the challenges and resilience of the modern digital society in August 2024. Our goal is to stimulate discussion about the state of cybersecurity and to share the lessons we have learned in recent years. In Finland, unfortunately, the role of the private sector in initiating initiatives has remained marginal. Think tank activities are limited in our country and there could be a wider demand for them. The white paper itself is therefore a convenient format for new ideas and initiatives. Our intention is not to criticise anyone, but to think out loud.

At first, with the help of the white paper, we would like to draw attention to the change caused by the war in Ukraine, not only in cyberspace, but also in our security environment more broadly. The paradigm of warfare has significantly changed. Various forms of hybrid influencing and harassment are increasingly taking place below the threshold of actual war, which poses multiple challenges that are difficult to answer. The picture of war has also changed. In addition to physical, so-called kinetic warfare, non-kinetic operations, such as cyber operations and psychological influencing in their various forms, such as fake news and other means affecting people's cognitive functioning, have emerged. The war in Ukraine is the first war of the digital and social media era in Europe. Its lessons will certainly be reviewed in the years to come and afterwards after the end of the war. It is also important to learn on the fly, already when the crisis is ongoing.

Second increasingly important key message is the protection of society's critical structures, so-called critical infrastructure, from various threats, including those from the cyber domain. Digitalisation and the Internet of Things are leading to an increasing connectiveness of critical systems to the computer network. Russia has been targeting these critical infrastructures and related systems by its kinetic and non-kinetic means in Ukraine. Cyberattacks have targeted the country's energy sector, telecommunications sector, media and logistics operators.

In order to prepare for threats arising from digitalisation, critical infrastructure should be defined. There are many, even hundreds, of definitions around the world. According to the EU, critical infrastructures include the electricity grid, the transport network and information and communication systems. In Finland, critical infrastructure has not been defined. When discussing critical infrastructure, and preparing for threats, special emphasis should be placed on its core: the electricity grid, digital infrastructure (especially telecommunications) and satellite systems that generate spatial data and precise time. Without these, modern societies cannot function. These structures are also interdependent on each other.

As a concrete proposal for action, we present that Finland should define the core of national critical infrastructure. It should be a part of national critical infrastructure and services, thereby improving overall management of critical infrastructure. Furthermore, a specific cybersecurity programme should be developed for this critical infrastructure, taking into account both non-kinetic and kinetic influencing in different stages of preparedness and incidents. The threat and risk awareness of critical infrastructure operators should be improved and measures to implement the requirements of EU regulation should be intensified.

Thirdly, in addition to taking into account the lessons learned from the war in Ukraine and critical infrastructure, attention should be paid in Finland to cyber management and cybersecurity of supply. This could mean, for example, clarifying the cybersecurity management model and management responsibilities. Currently, cyber expertise and management are dispersed across several

different administrative sectors. At the same time, this could mean establishing a comprehensive and long-term technology/security of supply programme in a non-kinetic operating environment and strengthening the national cybersecurity supply ecosystem and international partnership network.

Fourthly, protecting critical infrastructure and improving societal resilience cannot depend solely on the public sector. Measures should be discussed cooperatively in solution-oriented manner. By combining the lessons learned from the war in Ukraine, recognizing the importance of critical infrastructure, and improving cybersecurity management models and cybersecurity security, we will create a more cyber-secure society. In this respect, public-private partnerships have a key role to play. National cybersecurity requires extensive and close cooperation between authorities, the third sector, organisations and businesses. Cooperation can mean very different operating methods and forms, but clear structures and perseverance should play a key role in this. In concrete terms, cooperation could mean, centralised, reliable and cost-effective cybersecurity services for the public and private sectors, exchange of risk analyses and situational awareness, as well as analysis mechanisms or joint contingency plans to maintain cybersecurity of supply.

The development and improvements of cybersecurity do not happen by themselves overnight. The development of cyber risk analysis, clarification of management responsibilities, refining the lessons learned from the war in Ukraine, developing cyber management and security of supply, and cooperation between different sectors of society are important building blocks in the comprehensive development of cybersecurity in society. A long-term asset of Finnish society has been social trust between authorities and citizens. By taking this as a model also in the cyber sector, we can build a crisis-resilient society together. Concrete steps to this are set out in our white paper: https://www.cyberwatchfinland.fi/en/post/white-paper-challenges-and-resilience-of-modern-digital-society. ■

# MONTHLY REVIEW
# OCTOBER 2024

// Cyberwatch Finland Analyst Team

## CONTENT:



# IN THIS REVIEW

In this monthly review, we examine the most significant cyber phenomena of the previous month and tie them into larger topics. 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 themes whose development is worth monitoring.

In September, the cyber world focused particular attention on Israel's operations against Le-banon and Hezbollah, the further development of the cyber front of this conflict, and the use of cyber weapons at different stages of conflicts around the world.

Attention was also paid to the ever-increasing number of successful government operations against cybercriminals, inadequate private practices of technology companies, and changing guidelines on passwords. Of the phenomena to be monitored for October and the rest of the year, we would like to highlight the changes caused and required by the quantum transition and the acceleration of cyber influencing related to the US presidential election.

## 1. EVENTS IN THE CYBERLANDSCAPE

In September, the world was dominated by news of the flare-up of the conflict between the extremist group Hezbollah in Lebanon and Israel. The two sides have been waging a silent war for decades, but in September Israel escalated the situation into an active conflict, first with air strikes and a ground offensive that began at the turn of the month. Each conflict also has its own cyber front and competition for narratives in the information environment. One of the events that attracted the most attention in connection with this conflict was the explosion of pagers and walkie-talkies used by Hezbollah. Although it was not actually a cyberattack, cyber influencing is also part of the background to this operation. The reason why Hezbollah used this outdated technology in the first place was because of Israel's cyber deterrence, i.e. the fact that Hezbollah leadership was plagued by legitimate concerns that Israel would be able to use advanced means to spy on and monitor mobile phones and communications via them. While in principle, a step backwards in the level of technology can be an effective way to protect against cyber influence, in this case it led to bad consequences due to a lack of supply chain security.

The conflict is strongly visible in the information environment. Israel has sought to present its air strikes and ground offensive, which have claimed civilian casualties, as a mandatory measure to prevent a larger conflict. It is also justified by the objective of enabling civilians evacuated from northern Israel because of the threat posed by Hezbollah rocket attacks to return home. This has been done in order to justify otherwise questionably aggressive action. As always in information operations, the goal is not to convince the whole world, but to influence a specific audience. Israel's probable objective is therefore to convince states and others who are already sympathetic to it of the rationale for the operation, and to give them a reason to continue their support. On the other hand, the Israeli operation has been heavily criticized in several Western media. In particular, the damage it causes to the civilian population and its indifference to civilian casualties have been highlighted. The idea of preventing conflict through an aggressive operation has not been swallowed up either, but the goal of pacifying one front with a show of force is seen behind the operation. On the contrary, it has been estimated that escalating the situation could even increase the likelihood of a major war covering the entire Middle East.

The war between Ukraine and Russia has taught us that the use of cyber weapons is at its most intense just before a physical conflict begins. As conventional weapons start being used, the role of cyber influencing changes to intelligence gathering in the background and harassment of the opposing party. Hezbollah itself has not really played a significant role in the fighting on the cyber front, but instead, Iran, which supports it, has been involved in a cyber conflict with Israel for years. Since Israel began operations against Hezbollah, relations between the two countries have further escalated from the struggle in the cyber world to the level of missile attacks. In the conflict in Ukraine, the parties soon realised that cyber influencing is less applicable than expected to support physical war operations or achieve destructive effect. For example, cyberattacks on critical infrastructure were largely replaced by more effective missile attacks. In the context of the war in Ukraine, cyber weapons have been used since the beginning mainly to support intelligence and information gathering and, more recently, also in attacks on supply chains. However, the distance between Iran and Israel is still longer than between Ukraine and Russia, and cyber influencing may remain a more important tool than the comparison case. Iran's efforts to avoid escalation are certainly also behind this: cyberattacks can be carried out in such a way that their perpetrator is not revealed.

## 2. IN THE SPOTLIGH

### 2.1. Successful operations by authorities underline the importance of communications security

In September, Europol and Eurojust, together with the authorities of nine different countries, carried out an operation which resulted in the dismantling of the Ghost communication platform, which had been used by criminals. In total, 51 people were arrested, drugs and weapons seized and more than one million euros worth of cash were seized around the world. In addition, the servers operating the platform and the drug laboratory linked to the platform were shut down. This is a continuation of previous successful operations carried out globally by Western authorities. The Ghost system was a platform founded in Australia in 2015 with a custom-made Ghost phone at its core. The device was designed and manufactured specifically for use by criminals, as it was marketed as a guaranteed product whose communications would not be accessible to the authorities.

The background to this operation by the authorities was the successful penetration of the platform supply chain by the police. The authorities succeeded in modifying the system's automatic updates and thus gained virtually complete control of the platform. The operation highlights the authorities' growing ability to cooperate globally by carrying out demanding cyber operations that also have a direct impact on criminal activities in the physical world.

The success in dismantling the platform will surely raise growing concerns among criminals about their cybersecurity and the secrecy of their activities. Communications are often a weak point in cybersecurity, for criminals as well as everyone else. This also reminds the business world, the public sector and the third sector to focus more and more closely on the cybersecurity of communications. While criminal parties are vulnerable to law enforcement activities, we are also most vulnerable to criminal activity. In each organization, it is good to consider how one's own operations would be wounded if a third party were to gain access to the organisation's communications.

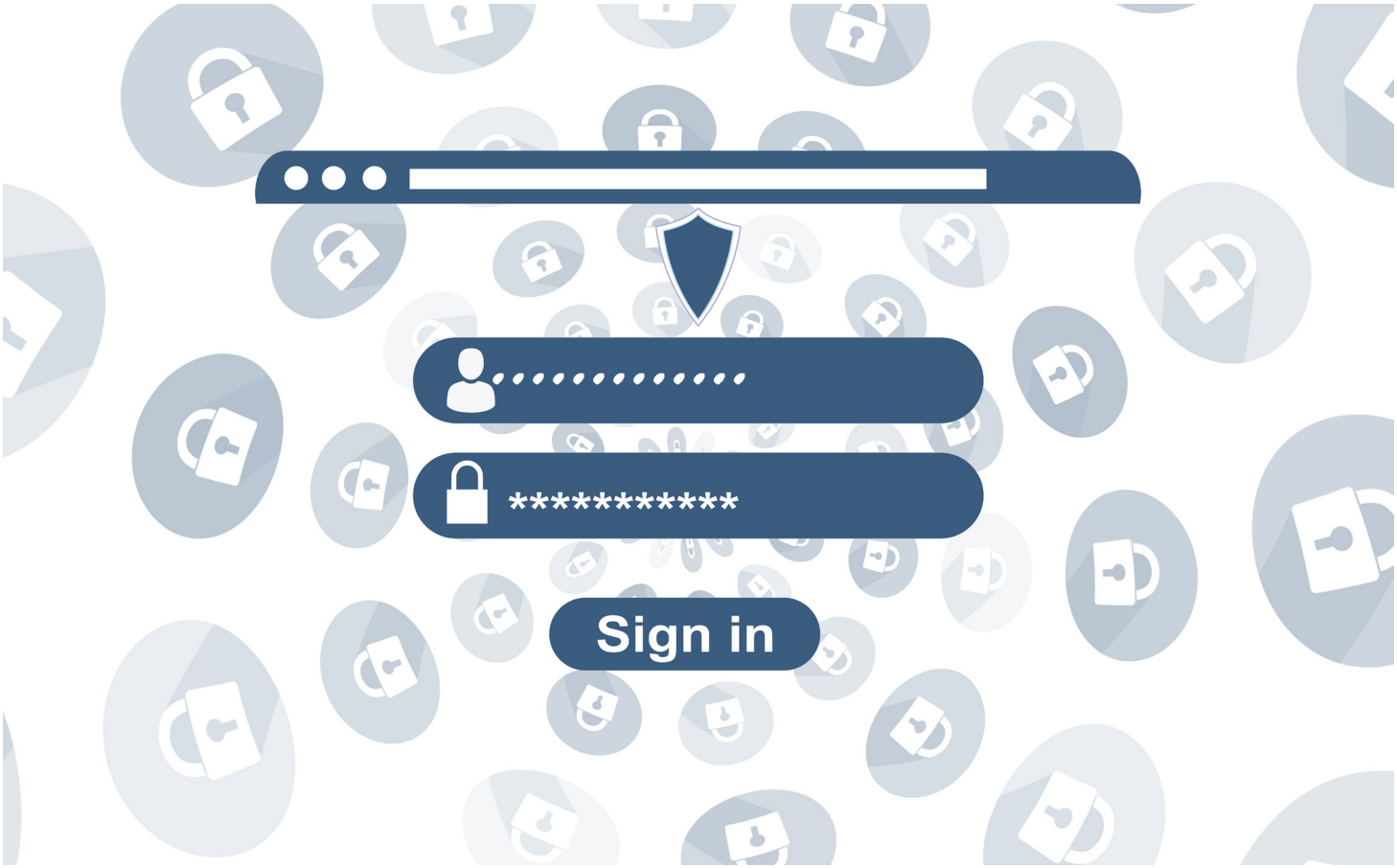
References on page 55


## 2.2. Technology companies and social media giants negatively in news in September

Big tech companies as well as social media platforms like Alphabet, Amazon, Apple, and Meta regularly make headlines for negative reasons. In September, the U.S. Federal Trade Commission, the U.S.'s consumer protection authority, published a report that it had been preparing for more than four years has on deficient practices by social media operators and video platforms. In summary, the FTC found indications of shortcomings in the privacy practices of the services, tracking users from one site to another, inadequate protection of children and teenagers, sharing user information with third parties, and improper storing of user data, among other things. In Europe, large technology companies have regularly received fines, for example on the basis of the EU ś GDPR regulation. Most recently, in September, Meta received €91 million in penalty payments in Ireland for storing some users' passwords as unprotected plaintext in its systems. In addition to data protection issues, technology companies in Europe have been in the headlines in September due to Apple's tax problems and Google's suspected antitrust violations.

The difficulties of big business in reconciling actions with legislation or good practice on both sides of the Atlantic are striking on both sides of the Atlantic. They have also attracted much criticism for other reasons. In the wildest claims, social media companies and technology companies have even been speculated to pose a threat to democracy. Examples of this include fake news, hate speech and deepfakes on platforms, which are thought to have an impact on election results in democratic states. Furthermore, their addictive nature has been seen to affect children and young people in particular. Despite the often happening sustainability talk, the tech and platform giants seem to have been relatively reluctant to address criticism or raised issues seriously. This is also indicated by the continuous penalty payments – the companies prefer to act in violation of the law and later, if necessary, pay the compensation imposed.

It should be clear that new ways for supervising the activities of technology companies and social media services should be invented. One could even say that there is some consensus on this between civil society and political decision-makers. Based on September, new measures to supervies tech giants are unlikely to be forthcoming. In its report, the FTC recommended curbing data collection and abandoning tracking technologies. But when these are only recommendations, it is likely that they will fall on deaf ears. Global problems need global solutions. For example, cooperation between EU and US authorities, harmonisation of legislation, defining and closer monitoring the responsibilities of technology companies could serve as a means of addressing the problem. Ordinary users should wake up to the problem, too. If individuals themselves are not interested in their own data or rights, can it be required from large companies operating on the basis of market economy?




## 2.3. Evolving password policies

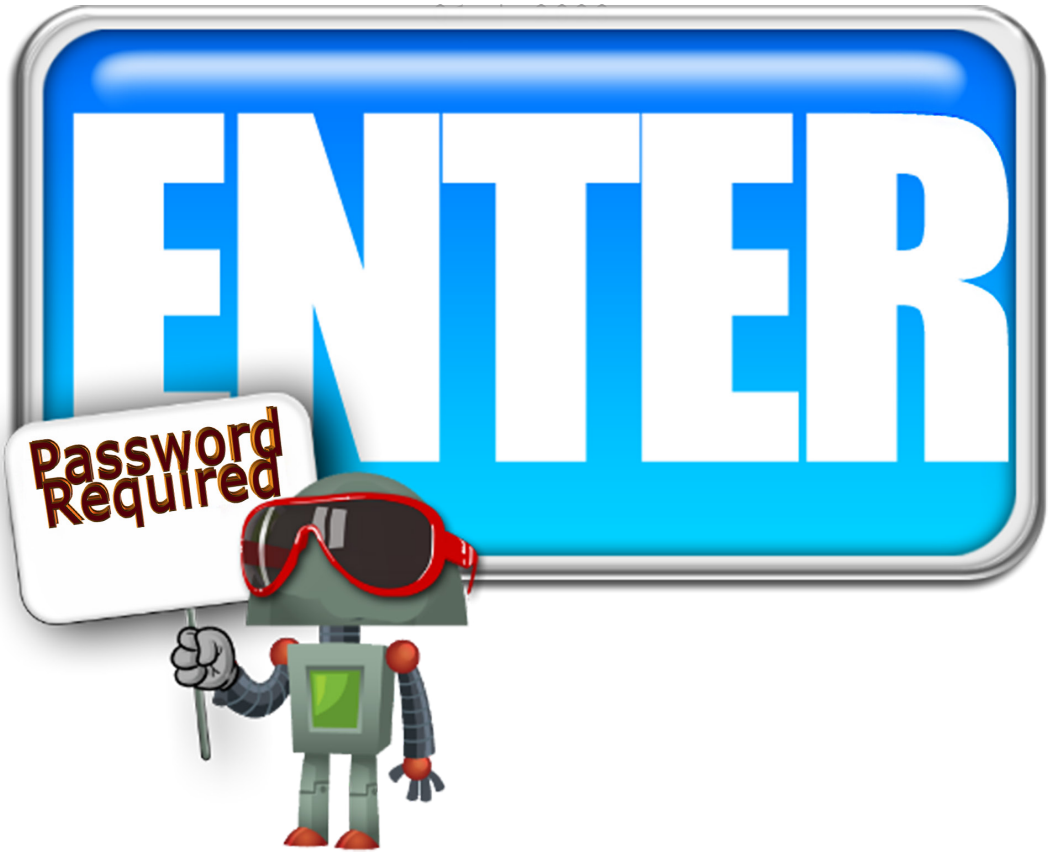
Passwords are a long-standing authentication method that has been found to be inadequate. They are often described as a poor but best available authentication option. Although replacement solutions are constantly being developed, passwords are still by far the most widely used solution. Problems with passwords do not focus on the technology itself, but on the people who use them. Their weaknesses stem from weak, reused, forgotten, or lost passwords. In almost every application, the security of passwords is improved by specifying what the password should be. Organizations often have guidelines or requirements related to the uniqueness of passwords or lists of prohibited words to maintain. However, people are bad at following instructions, especially if they feel hard and too much effort consuming. For this reason, guidelines for using passwords have to balance between security and ease of use.

At the turn of the month, efforts have again been made to develop password-related guidelines, this time by the National Institute of Standards and Technology (NIST). The agency has published new guidelines on what kind of passwords and related practices it considers secure, and how users should be instructed and supervised in their use. The NIST Guidelines will be implemented directly by at least a large number of U.S. government and government organizations and are also expected to serve as a guideline for the practices of private companies or organizations. The most important and interesting takeaways from the guidelines are the shift in emphasis from complex passwords to simpler but longer passwords, as well as the abandonment of scheduled password changes.

The first of these means that the instructions on what kind of characters passwords should contain are simplified and streamlined. Anyone who has registered a new service will be familiar with the fact that the service does not accept the password first offered, but requires that it contains, for example, both uppercase and lowercase letters, numbers and special characters. According to NIST, such requirements do not actually significantly increase password security, but rather the opposite. They lead to bad password practices, such as the use of the same or schematic passwords on different systems, forgetfulness or password sharing, and only extremely rarely do they provide the desired additional security against password guessing or hacking attacks.

In theory, including different characters in a password increases the password resistance exponentially to, for example, a brute force attack, but in practice this rarely happens. Usually, in passwords, special characters and numbers are not randomly included in the middle of the password, but almost always either at the beginning or at the end, so that the desired complexity is not actually achieved. Far more common than brute force attacks is password cracking by

References on page 55




guessing or exploiting commonly used passwords or other passwords for the same user. The NIST guidelines aim to modify policies to make it easier for users to remember their passwords and to prefer passphrases inside words. Multi-word sentences are harder to guess and easier to remember, especially when one does not have to mix them with special characters or numbers. Of course, the guidelines still allow the use of all different character types, and even encourage to add to allowed character types, but their use is no longer mandatory when creating a password. Only a password of at least eight characters should be required, but passphrases up to 64 characters long should be allowed.

NIST also urges the organization to abandon forced scheduled password changes. Forced password changes should be a method that is only used if there is a suspicion or knowledge that credentials have been revealed, for example, in a data breach or involve suspicious activity. In contrast, a forced password change every few months does not increase security, but, like complex requirements, only increases the likelihood of operating models that undermine security. In addition to these guidelines, NIST advises against password tips, or security questions that allow recovering lost passwords, as these can be easy to guess and, at worst, an easier way to break into systems than password snooping itself.

Thus, NIST seems to share the view of many experts that the more complex the requirements for passwords, or the more often they have to be reinvented, the more likely it is that the passwords in use are bad in some way. The idea of favoring longer passphrases over complicated short passwords or giving up forced changes are not unique ideas, but suggestions for improvement related to passwords raised by many others. However, NIST notes that this is in any case a weak solution, vulnerable to abuse and attack, that should be supported or replaced whenever possible by, for example, biometric or multi-factor authentication. NIST does not directly recommend the use of different password managers, although these are generally considered to be a relatively effective way to generate and maintain unique and durable passwords. The reason NIST does not recommend this option is likely to have more to do with the fact that their use requires an audit and trust in the service provider, rather than being bad. Password management software is inherently very attractive targets for cyberattacks, and NIST cannot generally recommend using just any provider's solution, as significant differences in security have been observed.

In any case, both casual users and those responsible for the organization's password policies should consider what kind of passwords or related requirements actually contribute to security, and which do not. The NIST guidelines can serve as a good starting point for updating the password policy. In addition to practices, it is also critical to gain visibility and detection of passwords that may have already been leaked, as even the most complex or longest password is not much more secure than 1234 if it is found on the dark web associated with a username.

The full NIST recommendations can be found here: https://pages.nist.gov/800-63-4/sp800-63b.html

## 3. FOLLOW THESE

### 3.1. As the US presidential election approaches, election interference intensifies

This year, as in the past, the US elections have been the focus of significant attention in the cyber world. Various influencing operations have already been seen and will be seen before the elections. Most attempts to have been various information operations aimed at influencing views on the candidates and the political agendas they pursue. Targeted cyberattacks against candidates or their campaign teams are less frequent. However, we have already seen them, and attempts have been made, for example, to hack the email accounts and other accounts of candidates and their staff and publish the messages they contain. Election websites have also been targeted by distributed denial-of-service (DDoS) attacks. Their aim has been to disrupt elections and make it more difficult to obtain information. In the end, however, the attacks have not yet disrupted the safe conduct of the elections.

The most visible election-related cyber operation occurred in August, when the campaign of Donald Trump, the Republican presidential candidate, announced that it had been the target of a cyberattack. At the time, an outside party had gained access to the emails of a politician close to Trump. The attacker then sent the hijacked emails to US media houses, which refused to publish them. Three members of Iran's Islamic Revolutionary Guard Corps have been charged in connection with the incident. The attack was carried out with a targeted phishing attack.

U.S. authorities have also announced numerous takedowns of fake news sites and various fake news campaigns. According to officials, the single biggest source behind fake news is the Russian state, especially its media companies such as Russia Today (RT) and affiliated actors. Russia has been accused of using artificial intelligence, bot networks and fake news sites to spread its own propaganda. In addition to Russia, fake news, disinformation and misinformation related to the US presidential election are spread by many other state-level actors, such as China and Iran. Actors inside the United States also unintentionally or deliberately spread various fake news and misinformation in the context of elections.

The authorities have taken a decisive stand on various influence operations and information campaigns. The aim is to avoid events such as the 2016 elections, when Russia, among others, was found to have spread a wide range of misinformation and disinformation related to the elections. In this case, the warnings and instructions issued by the authorities did not have time to properly reach voters before election day. Now the authorities have started in time to tackle all kinds of information campaigns for which there is no evidence of truth. In a democracy, however, it is very difficult to determine the level of misinformation and censorship. To what extent is it right to remove misinformation or misleading information from the web, with regard to freedom of expression and the right to express one's opinion. This balancing act is extremely challenging and should be assessed in the context of the US presidential election and the political debate surrounding it.

As the United States is one of the most significant and largest democracies, its elections are closely watched around the world. The information and cyber battle taking place in connection with these elections appears to the whole world as an example of what people are prepared to do in connection with the elections. The aim of authoritarian states, in particular, is to create mistrust in the democratic system in general and to create strong discord and polarisation within nations. Information influencing can be avoided quite well with media literacy, i.e. by taking a critical view of online content. In addition, it is a good idea to report incorrect information or, for example, fake news sites to the authorities or site operators, who then try to stop the spread of this false information.

References on page 55

## 3.2. Quantum-protected standards are ready and implementation can begin

The threat posed by quantum computers has been known and concerned for decades. In practice, the concern is related to the fact that when a sufficiently powerful quantum computer turns from theory to reality, its computing power can be used to break all the encryption technology currently in use. It is only a matter of time before this happens. Expert estimates range from years to decades. Since the threat is both serious and well known, efforts have been made to prepare for it for some time. The solution is considered to be new kinds of encryption algorithms that, unlike those currently in use, would also withstand the attack of a future quantum computer. Encryption algorithms are complex mathematical processes that render data stored in or transferred between information systems unreadable without the right decryption keys. In this way, information is encrypted from outsiders. The development of new algorithms is slow, and the transition to them is a long, multi-year process. So far, preparedness for a quantum threat has mainly been limited to awareness of the threat and discussion and reflection on what kind of algorithms would be best for responding to the quantum threat.

One of the actors whose done most concrete things for the quantum transition is the National Institute of Standards and Technology (NIST). In a process that has been going on for about eight years, NIST has collected, tested, and improved its proposals for potential quantum-resistant encryption algorithms with the goal of producing standards by which information systems could be secured in the future. Now, in early autumn, the first of these have been published in the form of standards FIPS 203, FIPS 204 and FIPS 205. The completion of NIST's work has been awaited around the world, and with it the first practical steps for the quantum transition can be taken. However, the transition will not be over overnight. Although there are still years to go before the threat materializes, NIST has called for the process to begin now. Some quantum-resistant solutions already exist, mainly implemented by private actors such as Google, Amazon and Apple in their own products. Authorities or regulators responsible for a large-scale transition, such as ENISA in Europe, have been waiting for NIST standards. These are more tested than commercial peers and designed to be compatible with the solutions currently in use, and a uniform standardized solution is also necessary for the future.

However, a trouble-free transition is not expected. Although the groundwork has been done carefully, it is still largely only theoretically tested solutions. It is likely that there will be gaps in standards or unforeseen challenges in coordination. NIST is also aware of the challenges and has prepared for them by announcing that it will publish new standards later this year and next year. These are intended to serve as a reserve in case the ones published now are broken or otherwise prove to be incomplete. However, according to NIST, practitioners should not wait for the reserve algorithms but start the implementation process immediately.

So who does the call to start the quantum transition now apply to, and what will the quantum transition require? Small and medium-sized operators need not worry, as for them the change will mainly be visible in the fact that at some point the systems and solutions in use will be updated to be quantum-protected in the next few years. However, decision-makers, legislators and those producing their own solutions should keep abreast of developments in the situation. Larger organizations need to start working on mapping all the data they need to protect and planning massive change. In Europe, organisations should also review their encryption practices, as they come with obligations in the form of the NIS2 Directive. ■

# REFERENCES


## EVENTS IN THE CYBERLANDSCAPE

Cyberwatch Finland Weekly Reviews of September
https://www.aljazeera.com/news/2024/9/24/why-is-israel-attacking-lebanon
https://www.csis.org/analysis/escalating-war-between-israel-hezbollah-and-iran

## SUCCESSFUL OPERATIONS BY AUTHORITIES UNDERLINE THE IMPORTANCE OF COMMUNICATIONS SECURITY

https://www.reuters.com/technology/cybersecurity/ghost-cybercrime-platform-dismantled-global-operation-51-arrested-2024-09-18/
https://www.europol.europa.eu/media-press/newsroom/news/global-coalition-takes-down-new-criminal-communication-platform
https://www.theregister.com/2024/09/18/51_arrests_ghost_platform/

## TECHNOLOGY COMPANIES AND SOCIAL MEDIA GIANTS NEGATIVELY IN NEWS IN SEPTEMBER

https://therecord.media/meta-unprotected-passwords-fine-gdpr
https://www.reuters.com/technology/eu-privacy-regulator-fines-meta-91-million-euros-over-password-storage-2024-09-27/
https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-social-media-video-streaming-companies-have-engaged-vast-surveillance
https://www.cnbc.com/2024/09/10/apple-loses-eu-court-battle-over-13-billion-euro-tax-bill-in-ireland.html
https://www.theregister.com/2024/09/19/social_media_data_harvesting_handling_ftc/

## EVOLVING PASSWORD POLICIES

https://www.darkreading.com/identity-access-management-security/nist-drops-password-complexity-mandatory-reset-rules
https://pages.nist.gov/800-63-4/sp800-63b.html
https://www.hivesystems.com/blog/are-your-passwords-in-the-green

## AS THE US PRESIDENTIAL ELECTION APPROACHES, ELECTION INTERFERENCE INTENSIFIES

https://www.nytimes.com/2024/09/04/us/politics/russia-election-influence.html?unlocked_article_code=1.PE4.B1C6.ZXLPVBRImUyl&smid=url-share
https://www.nbcnews.com/news/investigations/us-garland-indicts-three-iranians-trump-campaign-hack-rcna173001
https://www.state.gov/united-states-sanctions-iran-backed-malicious-cyber-actors-that-have-attempted-to-influence-u-s-elections/
https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/3994-odni-pr-22?
https://www.brookings.edu/articles/foreign-influence-operations-in-the-2024-elections/
https://www.cisa.gov/news-events/news/cisa-and-fbi-release-joint-psa-putting-potential-ddos-attacks-during-2024-election-cycle-context

## QUANTUM-PROTECTED STANDARDS ARE READY AND IMPLEMENTATION CAN BEGIN

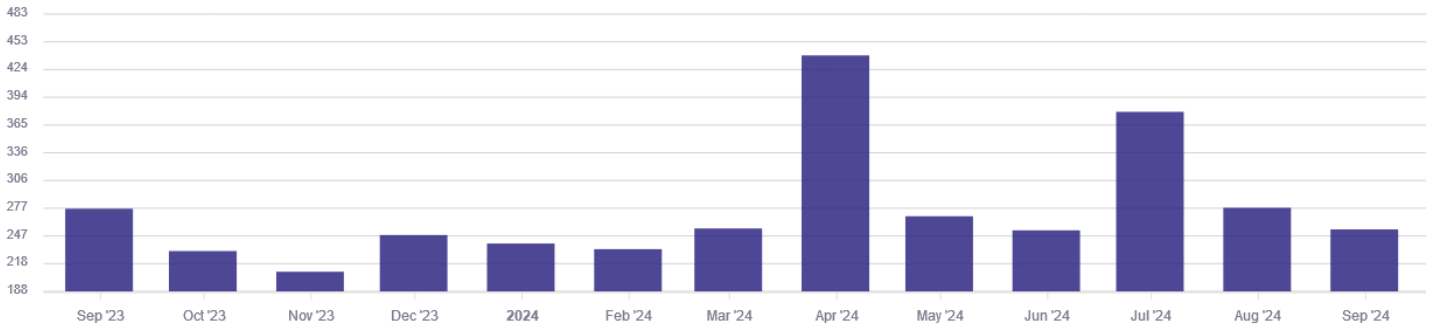
https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
https://www.technologyreview.com/2022/09/14/1059400/explainer-quantum-resistant-algorithms/
https://www.bleepingcomputer.com/news/security/nist-releases-first-encryption-tools-to-resist-quantum-computing/

Cyberwatch Finland

# 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.

# DATA BREACHES BY MONTH FROM LAST TWELVE MONTHS.




Source: Cyber Intelligence House

# MAJOR CYBERATTACKS AND CAMPAIGNS

## DUTCH POLICE

DATE: Incident announced 27.09.2024
DESCRIPTION: In late September, Dutch police reported being the victim of a cyberattack. The police stated that their personnel databases were targeted by the attacker who managed to steal an unspecified amount of police personal data. It was later reported that the attack was carried out by a state actor, but no specific accusations have been made against any specific target. No known hacker group has claimed responsibility for the attack. In the past, Dutch authorities have expressed concern about operations against the country, particularly by Chinese and Russian threat actors.
ACTOR: Unknown / state actor
MOTIVE: Unknown
IMPACT: Data from personnel of the Dutch police force, such as names, email addresses, phone numbers and, in some cases, other personal data, ended up in the attacker's possession. No information has appeared for sale or sharing, so it is unclear for what purpose the breach was made.

# MAJOR CYBERATTACKS AND CAMPAIGNS

## ALISA BANK AND SUBSIDIARY MOBIFY INVOICE

DATE: 03.10.2024
DESCRIPTION: The customer bulletin of Alisa Bank's subsidiary Mobify Invoice incorrectly included the email addresses of the entire company's customer base. The message, sent to thousands of bank customers, included the addresses of the entire delivery list. The bank has apologized and informed that it was a case of a human error.
ACTOR: Insider
MOTIVE: Human error
IMPACT: The disclosure of email addresses in itself does not pose a significant threat, but leaking the entire customer list can be useful, for example, for criminals who manufacture scams in the name of a bank. In addition, the transaction is embarrassing for the bank and will certainly affect customer trust. The magnitude of the reputational damage will only be revealed later, depending on customer reactions.

## RECORD-BREAKING DDOS ATTACK DETECTED BY SECURITY COMPANY CLOUDFLARE

DATE: September 2024
DESCRIPTION: In September, security company Cloudflare announced that it had detected and successfully countered a distributed denial-of-service attack (DDoS) attack that its customers were facing, touted as record-effective. The maximum power of the attack was 3.8 terabits per second (Tbps) and 2.14 billion packets per second (Pps).
ACTOR: Unknown
MOTIVE: The exact motive for the attack is unknown, but according to Cloudflare, organizations providing financial, internet and mobile web services were targeted.
IMPACT: While one of Cloudflare's motives for reporting the incident is to market and sell its own security services, the incident proves that DDoS attacks can be protected from when needed. DDoS attacks are a common cyber threat that has often been used by Russian hacktivist groups.

## E-COMMERCE GIANT TEMU'S DATA BREACH

DATE: 17.9.2024
DESCRIPTION: Temu, a Chinese e-commerce operator that is the subject of extensive social debate, was the target of a possible data breach in September. A sales announcement appeared on the hacker forum BreachForums, in which the advertiser announced that he was trading a package of more than 87 million records, including customer data.
ACTOR: A hacker or group of hackers trading data goes by the pseudonym smokinthashes.
MOTIVE: Financial
IMPACT: Temu denies being the victim of a data breach and has threatened lawsuits against those spreading "misinformation". The company said it had reviewed samples of the leaked data released by the hackers and said they did not match the data in the company's possession. Correspondingly, the threat actor assures that the data is genuine. The arguments put forward by either party cannot be reliably verified. In any case, the case highlights the risks associated with online stores and ordering from them, which can lead to leakage of personal data to the black market if data security is poorly implemented.

# ACTIVE AND GROWING THREAT ACTORS

## RANSOMHUB

DESCRIPTION: A ransomware operator first detected in January 2024 that acts as a RaaS service provider. The group takes a 30% commission from its subcontractors on all ransom income. The group's activities have been traced to several countries, including China, North Korea, Cuba, Romania and several CIS countries. The group targets countries other than those mentioned above in its hostile activities.
RECENT ACTIVITY: Activity increased steadily during the first half of the year, and the group was the most active in the past month with 75 reported victims. The group's latest victims include kitchen utensils retailer Domain Industries and assistive device provider Rollx Vans.
METHODS AND TACTICS: Uses both data destruction and encryption techniques in its attacks. The malware codes are Golang and C++ based. The group's malware code runs on Windows, LINUX and ESXi platforms.

## CACTUS

DESCRIPTION: A ransomware operator that has been active since at least March 2023
RECENT ACTIVITY: The group was the second most active threat actor in the past month with 26 reported victims.
METHODS AND TACTICS: The group exploits purchased credentials, partnerships with various malware actors, phishing attacks, and security vulnerabilities. Among other things, the group has exploited vulnerabilities in VPN programs. The group carries out double extortion, i.e. as a result of non-payment of the ransom, the victim's information is put up for sale or published online free of charge.

## NITROGEN RANSOMWARE

DESCRIPTION: A new ransomware operator detected in summer 2024. The group's victims are especially IT and third sector organizations in the United States.
RECENT ACTIVITIES: The group's victims have recently included a gaming company from Canada, an engineering firm from the United States, and a heavy equipment leasing service from the United States
METHODS AND TACTICS: The operations are based on malware embedded in Google and Bing ads. The victim is lured into downloading the malware, after which the attacker infiltrates the victim's networks and then carries out various data theft, cyber espionage and ransomware attacks.

## HANDALA HACK TEAM

DESCRIPTION: Iranian threat actor linked to the country's Revolutionary Guards. Considered one of Iran's most powerful hacker groups, often targeting Israel. The group became active in December 2023 and maintains several social media support collection and communication channels. Declared support for Hamas in the conflict against Isreal.
RECENT ACTIVITY: Recently multiplied its attacks on Israel and especially on the country's defense and military industries. In late September, the group announced that it had attacked an Israeli nuclear research facility, stealing about 200 gigabytes of data. The attack has not been confirmed by the authorities. The group itself announced the execution of the attack and is supposed to be in retaliation for the murder of Hezbollah leader Hassan Nasrallah in Lebanon.
METHODS AND TACTICS: The group carries out highly advanced and varied attacks against the Israeli regime and companies in the country. The aim of the attacks is not financial gain, but the group often publishes the captured data for free. The group has also been found to have exaggerated its attacks and sometimes even reported completely false cyberattacks. The aim is to influence Israel's ability to wage war and psychologically influence the population.

# A PASSION FOR A SAFE CYBER WORLD


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

# Our Mission: Make Cybersecurity a Business Opportunity

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

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

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

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

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

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

Aapo Cederberg, CEO and Founder, Cyberwatch Finland

# OUR SERVICES

## Management Advisory Services

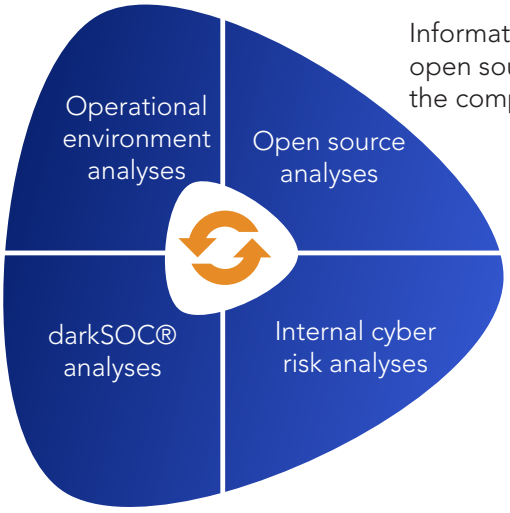
We are experienced and trusted experts and management advisors. We give support in comprehensive security, cybersecurity, internal security, and third party risk management. Our working methods include, for example, theme presentations, background memorandums, workshops, and scenario work.

## A Comprehensive Situational Picture

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

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

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




Information collected from open sources complements the comprehensive picture.

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

# OUR SERVICES

## Reviews

Cyberwatch's analysis team constantly monitors the cybersecurity operational environment by collecting and analyzing information about events, phenomena and changes in the cyber world. The situational picture is produced by regular situational reviews.


### Weekly Review

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

### Monthly Review

The monthly review sums up, expands, and puts into context the themes and phenomena discussed in the weekly reviews.
The monthly review describes of the development of phenomena, focusing on different perspectives of hybrid influencing.
With the help of the monthly review, it is possible to get a deeper insight into how the events of the cyber world affect society and the operational environment.
The monthly reviews are published 12 times a year in Finnish and English.

### Cyberwatch Magazine

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

### Special reports

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

# OUR SERVICES

## darkSOC® – the Dark and Deep Web Analysis

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

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


## The Benefits of darkSOC®

- Increases cyber intelligence capabilities
- Anticipipates constantly changing cyberworld
- Complements company's cybermaturity
- Serves as a forensic investigation tool
- Supports organisational strategic decision-making
- Complements strategic cyber situational picture
- Discovers vulnerabilities and weaknesses
- Fasilitates cyber strategy process

# OUR SERVICES

## Analysis

### The Surface Web Analysis

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

Powered by

Security Scorecard

### The Open Source Analysis

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

### Internal Cyber Risk Analysis

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

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

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

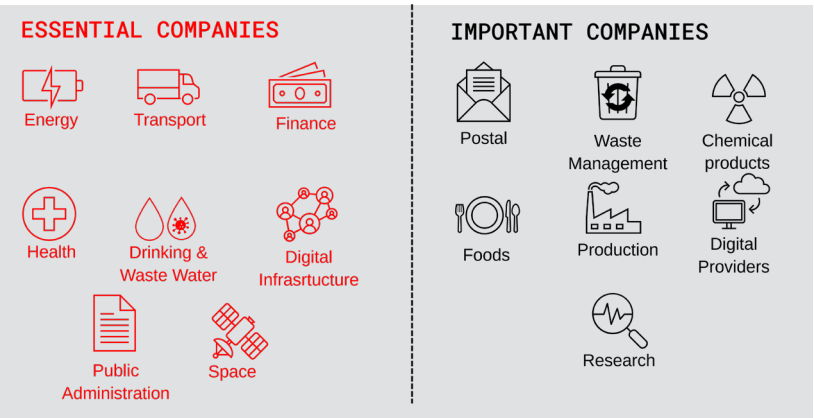
# OUR SERVICES

## Analysis

### NIS2 Consultation and capasity building

The aim of the NIS2 Cybersecurity Directive is to improve the basic level of cybersecurity in the EU and to ensure the continuity of operations of critical entities
The directive entered into force on 17.1.2023, with member states having time to put things in order by 17.10.2024.

### NIS2 cyber security directive concerns the following fields:




### The minimum requirements of the NIS2 Cybersecurity Directive are:

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

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

# OUR SERVICES

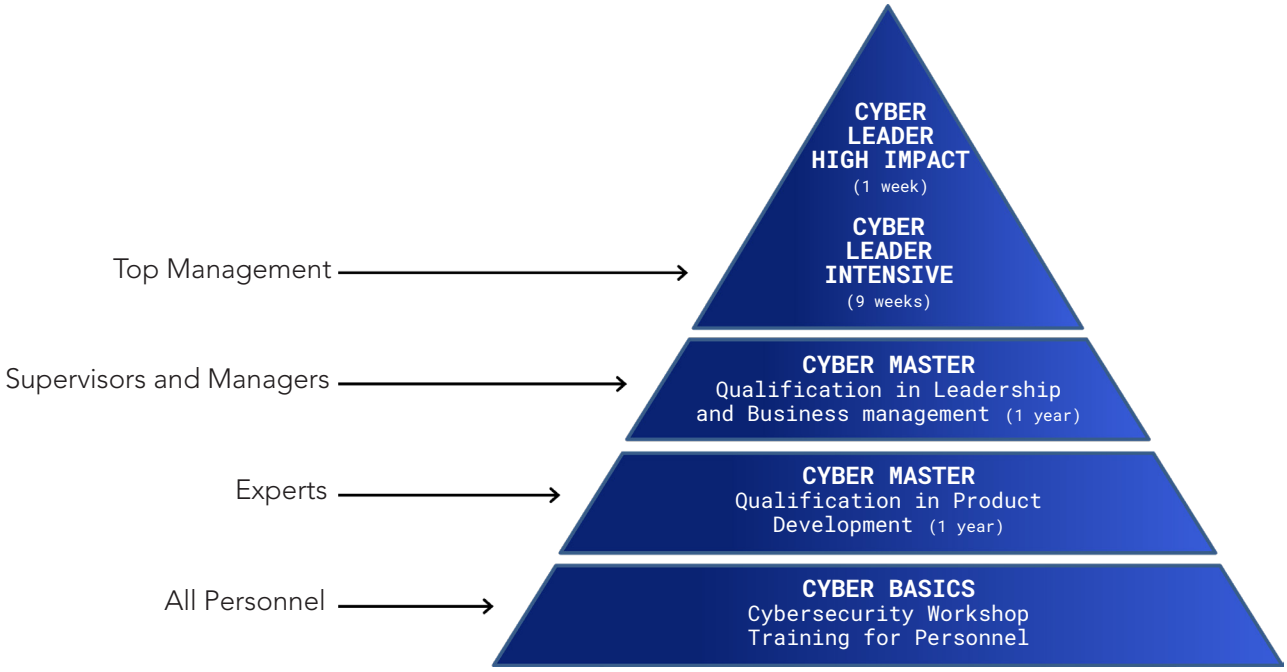
## Training and Competency Development

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

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

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

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





# A PASSION FOR A SAFE CYBER WORLD

## Contact

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi

CYBER SECURITY NORDIC

# Two stages packed with cybersecurity insights from leading companies and global experts

## AMONG THE HEADLINE SPEAKERS ARE:

**William H Dutton**
*Martin Fellow at Oxford University's Global Cyber Security Capacity Centre*

**Cybersecurity Capacity Building: The Whats, The Whys and The Hows**
Tuesday 29 Oct | 11:45–12:15

Prof. William H. Dutton, Martin Fellow at Oxford University's Global Cyber Security Capacity Centre is among the most interesting Keynote speakers. He was the founding director of the OII, the first Professor of Internet Studies at Oxford University, and an Emeritus Professor at the University of Southern California. His most recent book is The Fifth Estate: The Power Shift of the Digital Age (OUP 2023).

**Max Schrems**
*Lawyer, author, privacy activist NOYB – European Center for Digital Rights*

**Privacy in a global world**
Wednesday 30 Oct | 13:15–13:45

Max Schrems, a renowned privacy advocate and representative of NOYB – European Center for Digital Rights, will be among the notable speakers also in CSN 24. Schrems gained international recognition for his groundbreaking campaigns against Facebook (Meta), exposing privacy violations, including violations of European privacy laws. Noyb.eu has also recently filed a complaint against OpenAI with the Austrian DPA and is going to challenge the third attempt of EU-US data transfers agreement.

**JM Monteith**
*LM Fellow | Cyber, Lockheed Martin*

**The Evolving Threat to Critical Technologies**
Wednesday 30 Oct | 11:45–12:15

Mr. Monteith representing the US Lockheed Martin has 20+ years Cyber Security Architecture and Engineering experience in the Aerospace and Defence industry. Mr. Monteith has led enterprise initiatives in collaboration with, or in support of, Foreign Military Sales (FMS) customers, US and foreign government customers, partners, and suppliers, to develop, deploy and sustain IT and cyber solutions incorporating the full stack of information technology domains.

# Hacker's Corner – a new addition for 2024

A new feature at Cyber Security Nordic 2024 is the Hacker's Corner, where hands-on cybersecurity professionals are invited to test their skills in real-world scenarios and compete against each other. Participants will collaborate with leading cybersecurity companies to solve complex security challenges, diving into the mind of a hacker and tackling various puzzles.

**The participating companies offering the challenges are:**
**Trend Micro** – Focus on Red Teaming CTF | **Insta** – Intruders-demo | **WithSecure** – "Macbooks can't get viruses" | **Nixu** – Save Lucy from the dark! | **Vectra AI** | **Truesec**