TRAFICOM
Finnish Transport and Communications Agency

Strategic foresight

Cybersecurity scenarios 2035

Traficom's Technology and Strategy unit

Cybersecurity scenarios 2035

Contents of the scenario report

Cybersecurity scenarios 2035 – Background

- **Cybersecurity scenarios 2035** support the building of a cross-administrative model for continuous cybersecurity foresight and the creation of a cybersecurity threat assessment in line with the Finnish Cybersecurity strategy. The work on the scenarios started in autumn 2024 and was completed in spring 2026.
- A diverse group of more than 200 experts from the National Cyber Security Centre and its international counterparts, companies, academia, public administration and civil society were involved in the different stages of the scenario work.
- The cybersecurity scenarios 2035 describe alternative operating environments of cybersecurity. Stakeholders can add detail to and further develop the worlds described in the scenarios, for example in **sector-specific examinations**, and use them in **future-oriented training**.
- With the help of the scenario tools included in the appendix to this report, the scenarios can be used in **organisations' preparedness planning**.

Scenarios are tools for handling uncertainty

- Various key events in the operating environment today are taking us towards **different futures**. While we do not yet know what the world will be like in 2035, **we can try and prepare for it by perceiving possible trajectories of change**.
- The cybersecurity scenarios 2035 describe **alternative developments of the uncertainties in our external operating environment**. They offer a systematic way of understanding **different possible cybersecurity futures**.
- The scenarios are **alternative contexts for future decision-making, and by immersing ourselves in them, we can make better decisions with foresight**. They help us understand changes in the operating environment as a whole and anticipate the interconnections and interactions between various phenomena.
- The scenarios may seem more or less possible at the moment. **In 2035, the world will probably look like a combination of the different scenarios.**

Scenario process: Phases and elements

Drivers of change

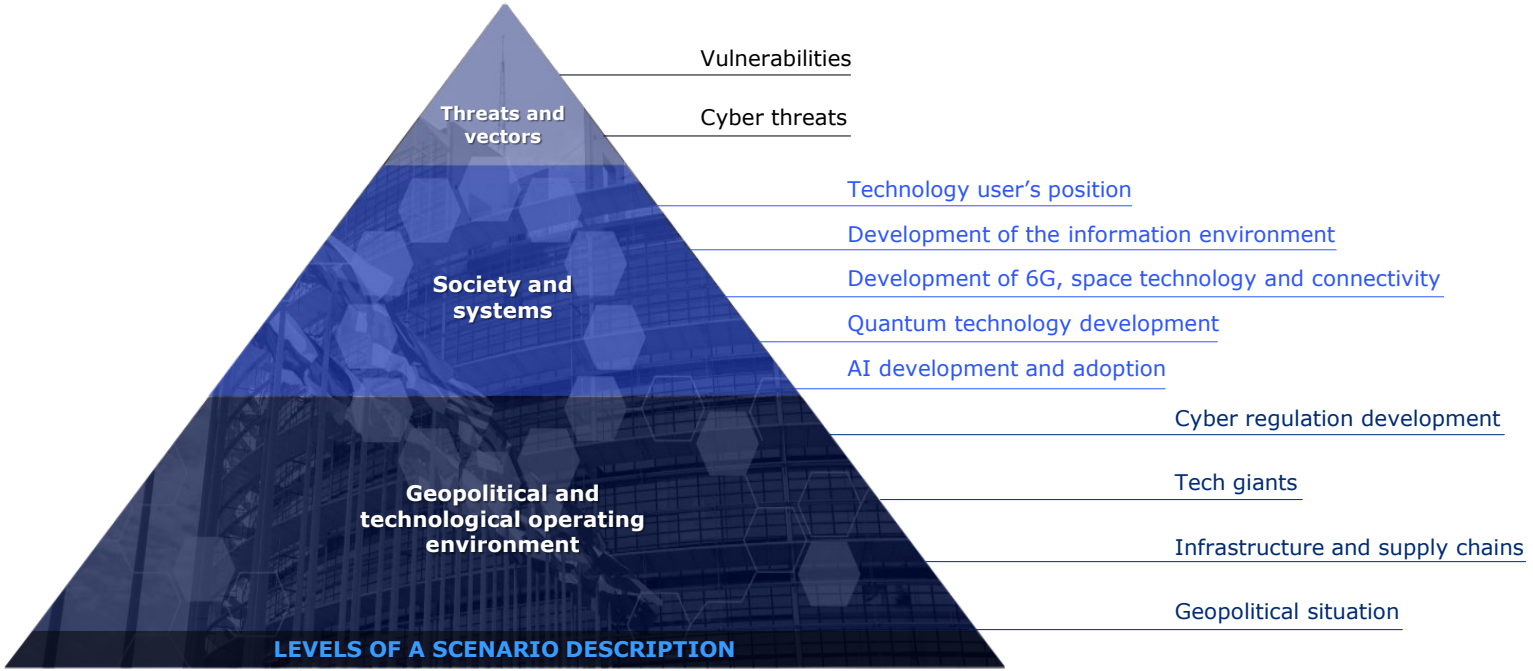
The drivers of change for cybersecurity identified in surveys, expert interviews and workshops may have developed in different directions and at different rates by 2035.	
Geopolitical development	AI & ML development
Digital infrastructure	Future of cyber regulation
Future cyber threats, including cybercrime	Information environment and society
Supply chains	Quantum technology
EU's unity and status	Power Tech Giants
Satellite and space technology	Organizational competence development
Organisations' preparedness solutions	Future vulnerabilities
Technological dependencies	Standards and trust
User behaviour	Disinformation and hybrid operations

How the scenarios were built

- The information acquisition phase consisted of four workshops with stakeholders, two scenario surveys targeted at stakeholders and 18 thematic interviews with experts.
- The scenario building phase consisted of four workshops with stakeholders and four in-depth interviews with experts.
- Using the *Futures Table* method, the scenarios were based on eight of the most impactful future drivers of change and their alternative projected developments.

Levels of scenario descriptions

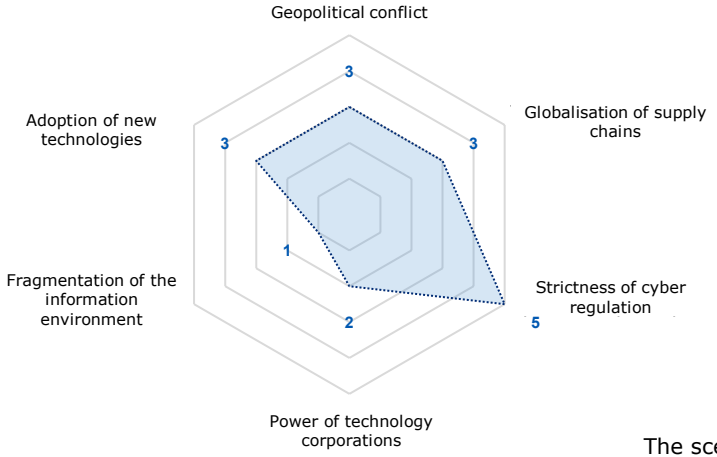
The cybersecurity scenarios 2035 describe four possible alternative worlds and their systems tinted by geopolitical and technological change, as well as the cyber threats and vulnerabilities that may emerge in these worlds of the future.



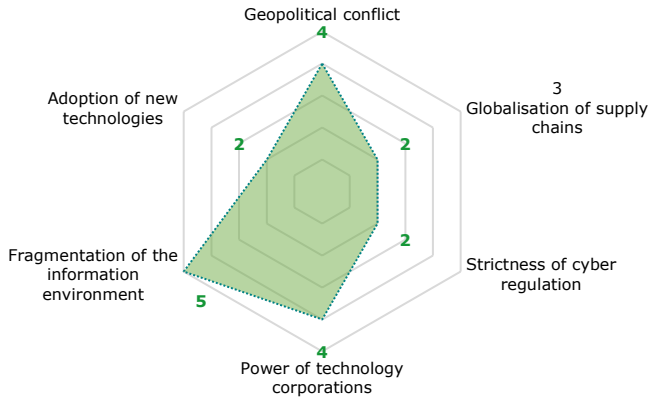
Cybersecurity scenarios 2035

Scenario descriptions

/TORCHBEARER/

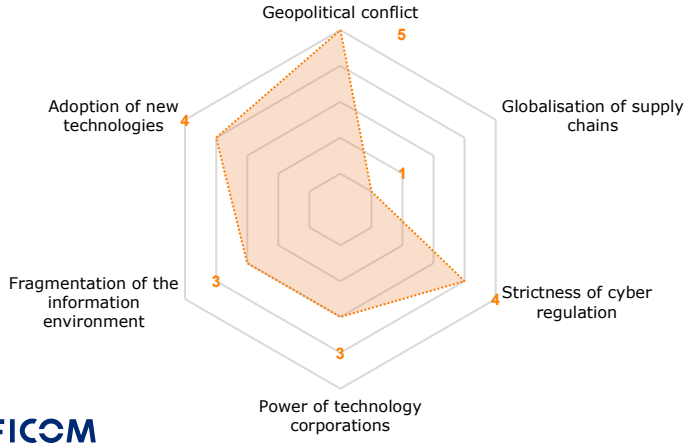


/FRAGMENTATION/

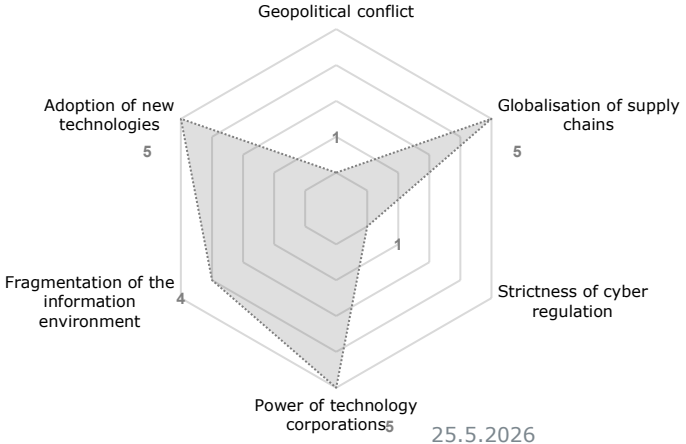


The scenarios differ in their features.
This optimises their performance as tools for examining new cyber security phenomena.

/TWO REALMS/



/DATA EMPIRES/



TRAFICOM

/TORCHBEARER 2035/

Confrontation between the major powers' spheres of influence persists.

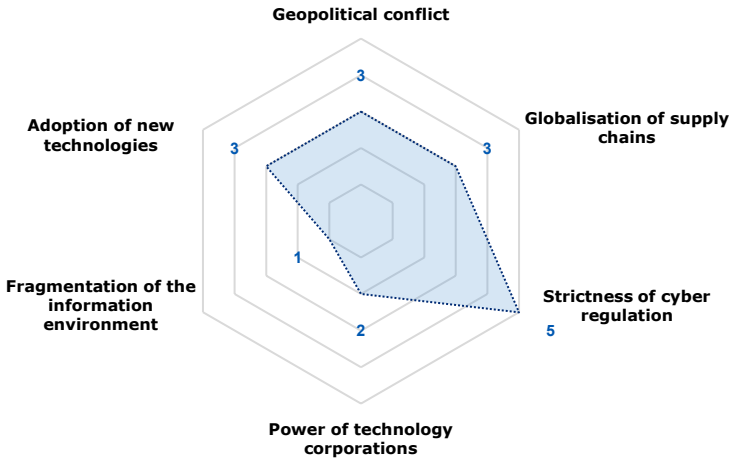
The United States has maintained its international lead over its competitor, China, but internal challenges and foreign policy excesses have driven it to become an ever **more authoritarian and unpredictable ally**. However, NATO cooperation and the Western security architecture remain strong, and **China and its BRICS allies have not been successful in challenging the West.** The EU has increased its strategic autonomy in relation to the United States while contributing to the alliance of democracies. **State actors continue to spy on and sabotage Western systems in anticipation of future conflicts.**

New technologies are introduced at a moderate rate.

LLM-AI development has not fulfilled the grandest promises, and some of the largest projects have been cancelled as unfeasible. Over-building of infrastructure, over-selling of solutions, legal challenges and data breaches have made financiers cautious, slowing down adoption and resulting in an AI winter of large models. **In parallel to the LLM development cycle, AI applications based on high-quality *organic data* and limited use cases have been developed** (incl. SLM models and edge device solutions) and successfully introduced in the EU. The interoperability of high-quality business data is advancing in leaps and bounds in the common market. **The EU has improved its self-sufficiency in cloud services, AI applications, quantum technology, 6G technology and space technology as well as its data sovereignty.**

Fragmentation of common understanding is prevented in the EU.

As platform companies are subjected to regulation, the EU is a model example of a citizen-centred and well-regulated information environment. Platforms have a regulatory obligation to ensure that the information they present is correct. The EU safeguards trust in society and a common foundation of information on platforms requiring strong identification. **Foreign operators are obliged to make their algorithms transparent** and expected to verify synthetic and organic content. Built-in AI-generative service designs in personal devices work as an unobtrusive way to guide users to operate securely, while official information environments are also accused of censorship.



Politicisation erodes the power of Big Tech companies.

Global tech corporations pick their geopolitical reference groups and become parties to the competition between the major powers. In order to broaden their customer bases, it is in their interests to expand China's or the United States' sphere of influence. **However, politicisation has eroded tech giants' reliability, as a result of which they have to make concessions in compliance with EU regulation** and operate more locally in order to continue their data and platform economy activities and to hold on to their markets. The EU ensures that they do not get access to greenfield companies working on cutting-edge technologies or valuable, specialised data.

Friendshoring & de-risking continues.

While global supply chains centred on China have remained the key channel of the world economy, **China and the United States have restricted the use of each other's services and infrastructures.** While the use of Chinese technology has been banned in many EU countries in the core areas of critical infrastructure, Chinese services and devices are more prolific in the consumer market. **The EU has stepped up its cooperation with Western countries and maintained neutral trade relations with China and the BRICS countries, with the exception of Russia.** Possibilities of improving trade relations with the largest economies in Africa, among others, are being investigated. Russia has been formally reintegrated into the world economy on the United States' initiative, but its relations with most EU countries have remained tense.

More stringent cyber regulation is brought in.

The EU is a leader in technology and cybersecurity regulation and creator of standards. **Supported by a strategic bid for autonomy, the EU builds a regulatory environment for AI applications and data use which upholds democracy and privacy and to which international tech companies are forced to adapt.** The EU cloud environment is based on strong user identification, ensuring a minimum level of regulatory information security. In the Western countries, the predominant trend is that the value of the data to be protected determines the priorities of security in practice. Companies have an incentive to comply with information security regulation when it comes to valuable and verified *organic data*.

Confrontation between the major powers' spheres of influence persists

Geopolitics and the world economy are going through an era of deals made with the United States while China's competitiveness is approaching the US level. The United States has been hit by *financial crisis Dotcom 2.0* as the LLM and AI bubble inflated by tech corporations has burst, and the international position of companies in this sector has weakened. **However, the US has simultaneously managed to hold on to its relative leadership position by turning third countries against China with bilateral agreements**, as China is increasingly seen as a creditor rather than a sponsor. Instead of direct geopolitical confrontations, **a competition for technology, allies and natural resources is underway to prepare for possible conflicts**. A steady stream of actions that are just short of open warfare characterise the relationship between the major powers and their spheres of influence.

Heightened tensions between India and China have reduced China's geopolitical room for manoeuvre, and BRICS cooperation has not taken a more concrete form as the member countries hold their own against China's economic dominance, with the exception of Russia. **Russia has partly reintegrated into the global economy** in the energy and raw material markets. The relationship between the EU and Russia has remained tense.

While the **United States has** become an increasingly autocratic and unpredictable ally as a result of its internal challenges, it has – **despite its protectionist antics – upheld its commitment to NATO cooperation** among other things. The EU and its partners in the Commonwealth countries, Japan and South Korea have become desensitised to the United States' protectionist impulses, and using technological and economic sticks and carrots has become commonplace in world politics, even between countries that are formally allies. Other Western countries are striving to reduce their technological dependencies on the United States wherever possible.

Friendshoring & de-risking continues

Global supply chains revolving around China have remained central in the world economy. China and the United States have strongly restricted the use of services and infrastructure supplied by each other's companies. The United States increasingly demands that its allies break away from Chinese infrastructure and services. Whereas Chinese technology is indeed banned in many EU countries in the core areas of infrastructure, Chinese services and devices have proliferated in consumer markets. **The EU continues to be largely dependent on US technologies while it strives to keep individual freedoms and privacy at the centre of the digital transformation.**

With large US corporations' reduced room for manoeuvre, the European Commission has identified an opportunity for repatriating critical data and improving the EU's self-sufficiency, especially in the form of sovereign cloud solutions. The EU's public cloud ecosystem protects citizens' sensitive data and manages the most critical information systems from its own sovereign data centres. Companies have formed data pools based on accumulating sectoral data, and corporations outside the common market pay a fee for using them. **The EU has introduced electronic eID identities and controls their access management.**

The EU common market has boosted companies' growth, and data interoperability is advancing in leaps and bounds. However, achieving overall digital sovereignty proves difficult for the EU, even if trust in the United States and its companies has eroded. The EU's sovereign cloud capacity mainly covers the most sensitive processing platforms used alongside US hyperscale environments, which process other data in compliance with regulation.

More stringent cyber regulation is brought in

The EU has kept its lead in technology and cybersecurity regulation and the creation of standards. Supported by a strategic bid for autonomy, the EU is striving to build a 'third way' of digital and cyber regulation, which refers to a regulatory environment for AI applications and data use that upholds democracy and privacy, with hopes of turning it into a counterbalance for Chinese and US systems with a global impact. The regulated EU cloud environment ensures a minimum level of compliant information security and data protection for citizens.

Despite more stringent regulation, a tendency for companies to balance between regulatory compliance and risk-taking is prominent in the Western countries: **the value of the data to be protected determines the security priorities in practice.** Companies have an incentive to comply with information security regulation, especially when it comes to valuable and verified *organic data*, and safeguards are developed especially for areas where a potential leak would lead to a higher price tag on the penalty. A privacy data exchange sets a price for data in regional, like-minded geopolitical peer bubbles, and Western countries as well as Digital Belt & Road states end up with their own variations. **The privileged can hold companies accountable and pay for their security, whereas more risks are taken with regard to other population groups' data protection in practice.**

Regulatory control and communication function between the authorities within geopolitical regions, such as the Western countries and Digital Belt and Road countries. Cooperation between the spheres of influence has declined. EU funding bodies gain more influence in the management of strategic self-sufficiency.

Politicisation erodes the power of Big Tech companies

As a result of global protectionism, large tech corporations are forced to choose their main geopolitical reference groups and markets between the United States and China. They consequently have an underlying interest in helping to expand the major powers' geopolitical spheres of influence in order to broaden their potential customer bases. **However, politicisation has eroded the reliability of large tech corporations, increased resistance and improved the position of local competitors**. As a result, tech corporations are forced to make concessions to EU regulation in order to fully continue their data and platform economy activities in this region.

The EU ensures that large foreign corporations cannot get hold of information on technology sector greenfield companies or valuable, sector-specific specialised data. Corporations are forced to balance between maintaining the trust of the EU market and citizens as well as promoting the political objectives of their parent countries, nevertheless leaning towards the former option.

AI: Low-level autonomy, high-quality data

The first wave of LLM applications cannot be made profitable, and **overbuilding infrastructure, overselling solutions and the collapse of expected returns have led to financiers withdrawing their investments**. The manipulation problems and hallucination associated with the largest models have not been solved. The volumes of AI-generated content and synthetic data are larger, but they cannot be used recursively to develop the models further. Authentic and quality-assured *organic data* has increased in value. Models that prioritised scaling have been proven the wrong approach to reliable and autonomous AI technology. As volume-based development has turned out to be unprofitable, the availability of processors and graphics cards has improved. Computation is increasingly shifting from large cloud implementations to more limited tasks and local edge device computing. The LLM wave has made room for an SLM wave. **AI is a tool among others, that enhances coding and software development in particular**.

EU language models with high-quality training data have found their place in citizens' everyday use, but the **employment impacts of technology are limited due to the restricted autonomy of the tools**, and quality assurance by humans is still needed in processes. The most important application areas are **modelling and real-time analysis based on big data**, for which EU companies create sectoral data pools.

AI agents linked to low-autonomy eID identities are able to manage everyday tasks and have made a breakthrough in the EU, however with restrictions that limit their access rights and give operators an unquestioned right to override them.

Encryption algorithms win the quantum race

Sensitive data are secured with quantum-resistant safeguards. The EU has kept up with the United States and China in quantum infrastructure building by supporting business ecosystems in the common market, and quantum-resistant protection has been built in key parts of critical infrastructure. The first solutions for breaking traditional cryptography have been developed, but encryption solutions have developed faster than decryption methods, and the greatest advances mostly comprise information influencing. **The EU uses advanced encryption solutions to protect data such as the connected EU business ecosystem data and citizens' personal data.** Decryption of previously collected data with lower-level protection becomes possible for state actors, forcing organisations to accept the fact that old data becomes public and the risk management measures that follow.

Western cooperation improves connections

Globally standardised 6G is deployed rapidly in the 2030s, and **in addition to EU Member States, a large part of the hardware and software come from the United States, South Korea or Japan**. **Fast broadband connections in remote regions of the EU are mainly implemented by the EU's IRIS² constellation, with US service providers supplementing the capacity.** Telecommunications operators, cloud computing platforms and logistics companies integrate satellite services into their offering through API-based partnerships with ecosystems operating in the EU that have some external dependencies.

The **compute overcapacity** built in connection with the LLM hype **is harnessed for building real-time and realistic remote connections where applicable. VR realities supplied by companies in the EU internal market are commonplace in organisations.** The connectivity of societies has led to a diverse combination of sensors and interfaces. **Digital twins that run, enhance and monitor industrial, economic and societal systems have become more common in the EU.** The technological configuration is made more complicated by subcontracting chains where some of the service packages are supplied by non-EU operators, as the systems have no direct visibility of the components maintained by them.

Fragmentation of common understanding is prevented in the EU

Concerns over a fragmenting information environment and the collapse of the shared foundation of reliable information leads to political efforts to secure this foundation. **As a result of successful regulation targeting platform companies, the EU is a model example of an oasis-like, regulated information environment**. At its core is the maintained 'official information environment' that is located in the EU cloud and accessed with strong identification. **Citizens are guided to the environment through media education and advocacy**.

Regulators impose an obligation on platforms to ensure that the information provided on them is factual. Foreign operators are obliged to make their algorithms transparent and expected to verify which content is synthetic and which is organic. As a result of increased use of generative AI, however, wastelands of synthetic data and disinformation, where platforms and state actors are striving to monopolise the truth, thrive outside the oases of curated data and information.

Affordable processors, graphics cards and computing capacity in the market have put capabilities in the hands of threat actors, leading to improved performance of deepfake technologies, among others. **To expand their spheres of influence, China and the Digital Belt and Road countries and, on the one hand, the United States and its closest allies are striving to build their stories of the world in their *spheres of information influence*, supported by synthetic content producers and population groups.**

Information security from the grassroots

EU users integrated with AI assistants enabled by strong identification are recognised as a high-risk combination of biometric and personal data, and platform functionalities are restricted in strong identification environments. **The list of permitted applications as well as sensors connected to eID virtual users and smart sensors grows shorter in the EU** to prevent information security risks. EU-compatible versions of devices are produced. Audits of latest innovations and getting them onto the common market take time, a fact which some users are not satisfied with. Agent deployment on platforms drives a need for stronger biometric identification, causing a division between the EU Member States. A set of digital norms is introduced in an effort to respond to citizens' increasing demands for authenticity, privacy and analogy. **The desire to manage one's own data, to consciously opt out of technology use and to consume content produced by humans gains ground.**

More stringent rules are imposed on advertising on social media and AI platforms, and data business restrictions mean that non-EU platforms are subject to fees. **Generative service design on platforms guides users to operate securely.** However, basing the EU's information environment on the premise of a single objective truth is not easy. **Official information environments are accused of censorship, and many feel that the 'EU reality' protecting users from disinformation is an authoritarian rather than democratic way of life.**

Some users **attempt to circumvent restrictions on applications and devices by obtaining them from unapproved sources. Through AI anomaly tracking in supply chains**, the use of illegal technologies, devices and platforms not covered by official user support with an eID identity leads to quarantining and restricted access to official services and, in the worst case, charges of espionage and spreading of disinformation.

Attack surface: Democratically sovereign infrastructure

- The EU's centralised strong authentication identity solution comprises a significant catalogue of citizens' sensitive biometric and other personal data accumulating in sovereign EU data centres.
- The second wave of AI competition highlights high-quality, private *organic data sources* that have been accumulated as the 'crown jewels' in sector-specific data pools of the EU common market.
- Due to the EU's bid for strategic autonomy, the electrification of the energy infrastructure has increased the potential of renewable energy, with an emphasis on smart grids which inevitably involve non-EU components.
- Increased IoT and IIoT connectivity requires large numbers of edge devices, especially in the Smart City configurations of the largest cities, where data on societal functions builds up in data mills and digital twins working to optimise these functions. The part visible to the citizens is linked to features such as navigation and traffic control through personal AI assistants, leading to better services.
- EU countries' verifiable and validated data are centralised to an information environment of verified data that is accessed through strong identification and that actively edits the image of the world conveyed to the citizens as a countermeasure to disinformation. AI assistants working through the common EU language model serve as personal verifiers and curators of the information environment.
- Because of the trend towards an ageing population, the EU has been unable to catch up on the number of required cyber experts, and there have been proactive efforts to recruit professionals from elsewhere to manage the attack surface. On the other hand, affordable processors and specialised models have enabled light-weight solutions for autonomous cyber defence.
- The requirement of strong eID identification and the limited range of applications in the EU prevent citizens from ending up with phishing copies of these applications coded by threat actors with AI assistance.

Threats: Operations just short of open warfare

- State actors spy on and sabotage Western systems in anticipation of future conflicts. Cyber campaining happens in short of use of force.
- Personal AI assistants as expressions of the EU language model can be programmed to surreptitiously influence citizens who have become dependent on them in their daily lives. The training data for the EU language model's assistant/agency applications are targeted by poisoning and corruption attacks.
- With precise limitations and assignments, AI tools can be used in attacks and defence. The more stringent AI regulatory environment and its security requirements slow down the adoption and development of defence applications, compared to attackers' unrestrained capabilities.
- Cybercriminals are interested in using the data combinations of EU cloud services – which have accumulated eID biometrics and personal data – for data breaches, scams and phishing. Attempts are made to access the systems through persons working with them.
- Attacks target EU Member States' information services, including statistical institutions, with the aim of accessing citizens' register data and reverse engineering it for the purposes of AI-assisted personalised attacks.
- The EU countries' renewable energy infrastructure is targeted by cyberattacks and sabotage aiming to reduce trust in renewable energy sources.
- The emphasis on *organic data* in AI/ML development makes companies' sectoral data attractive and valuable for espionage.
- The Smart City nodes of digital twins are targeted by espionage and sabotage. Crosspoints are used to break into individual sensors and data centres as well as to manipulate digital twins' AI interfaces.
- Phishing attempts aim to manipulate citizens who are keen on the latest innovations and applications in order to connect illegal devices and applications to their eID users and societal systems.


/FRAGMENTATION/

/FRAGMENTATION 2035/

Crises slow down the adoption of technologies.

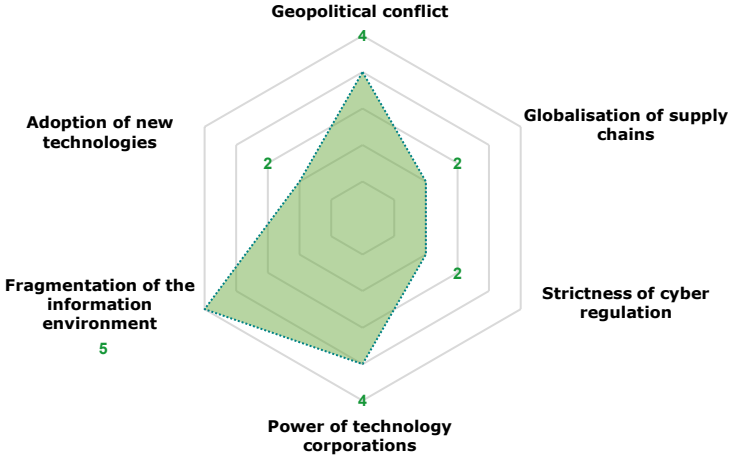
The AI interfaces and insecure and poorly maintained LLM-coded solutions deployed by companies due to the influence of large tech corporations have provided large-scale access to sensitive information in various **'AI disasters'**. Applications deployed in societal structures have been tweaked for use in espionage, disinformation and manipulation in democracies, and the **data collected by them have been successfully reverse engineered to identify individuals and organisations' sensitive data**. Organisations are forced to produce significant risk assessments when deploying AI tools, and the solutions used are often narrow but, **in terms of privacy, the damage has already been done**. Technological standards such as 6G have diverged strongly. Mistrust in US technologies slows down the introduction of new technology and drives some countries to the Chinese camp, **leaving the EU with a patchwork infrastructure**. It is hoped that quantum-resistant encryption solutions will restore trust in society, but the EU is lagging behind in its development.

Nothing can be trusted.

The usability of the public Internet has crumbled as AI-generated synthetic data and interaction have taken over, and users have turned to closed communities and networks in order to escape this trend. Data leaked from smart systems have been used to blackmail individuals and companies, legal challenges are more numerous and attitudes towards data disclosure more negative, reducing the availability of AI training data. A variety of worldview-shaping truths are found on different service providers' platforms. Demands for stepping back from the information environment filled by digital pollution have increased. **Citizens' communities are introducing methods of poisoning and scamming sensors and smart features, such as *Nightshade***, in order to escape companies' and authorities' algorithms and tracking.

The world is adrift.

The United States has turned its back on international cooperation forums and focused on its immediate national interests. Authoritarian states are spreading their influence by **attempting to drive a wedge between the EU and democracies by aggravating their internal and mutual conflicts**, as well as through economic incentives. Populations are divided into groups living around large corporations' technologies and those opposing technological globalisation. Formulating common positions has become more difficult, weakening the EU as a regulatory body.



Big Tech dependencies grow despite the mistrust.

Large tech corporations compete for users, data, energy and market areas without major barriers. China's growing sphere of technological influence hampers the spread of Western solutions, and the shrinking market area forces Western companies to shore up their position in democracies' public administrations. They take on a stronger role as quality controllers and maintainers of digitalisation in societies, also gaining political power in return, while encountering wider opposition and a tendency to opt out in some population segments. **Only their specialised subcontracting and supply chains** along with ecosystem identity management services can guarantee the digital continuity of societies.

Supply chains and EU infrastructure decentralise.

Challenges in the availability of technology make it difficult to maintain the information society, and in its efforts to ensure continuity, the EU is at the mercy of the parties controlling large supply chains. In terms of their economic and security interests and as a result of lobbying, the Member States are divided into camps that favour either American or Chinese solutions, preventing the formulation of a uniform infrastructure policy. This results in **fragmented digital development in the EU**, in which Western European countries make procurements from the United States or other Western countries, or build joint solutions. **However, Eastern European countries are striding ahead, boosted by China's Digital Belt and Road integrated technology and infrastructure.** Due to the declining ability to manage **supply chains**, insecure devices and vulnerable information networks have become more common.

Regulation cannot cope.

The public administrations of a growing number of countries are 'collapsing' digitally, as decision-makers cannot master the unpredictable big picture of technologies along with its risks and dependencies. Large corporations succeed in preventing regulatory efforts in democracies, staying at the forefront of technological development that only the corporations themselves can understand. **Internal blocs hamper EU decision-making as the number of divisions has grown and the Member States have divided into smaller interest groups, paralysing the Commission.** In a volatile operating environment, efforts focus on acute security issues, and protecting ordinary users from external threats and the corporations' vagaries is overlooked. Citizens' ability to enjoy basic digital security guaranteed by regulation is undermined, and EU Member States can no longer guarantee it for those in the lowest income brackets.

The world is adrift

The United States has turned its back on international cooperation forums. The burden of its military interventions and instability created by an escalated economic crisis have driven it to focus on its immediate national interests, making alliances transactional. **In an era of multipolar fragmentation, China and its allies fill in power vacuums.** The global rules are being renegotiated. The United States and China engage more frequently in high-handed policy that threatens sovereignty, which leads to limited regional conflicts affecting Europe and Asia and the use of various economic weapons, undermining global supply chains and access to technology.

Following the AI revolution, Europe has woken up to a situation where **applications have not fulfilled the promises of efficiency without a significant increase in security problems**. **Injudiciously deployed and developed LLM-AI applications and interfaces deployed have inadvertently enabled broad access to sensitive data**. As a result, political influence and social control has shifted to outsiders through user interfaces and the reverse engineering of collected data. Autocracies have protected their citizens from foreign technology but **applications widespread in western democracies have been tweaked consciously and unknowingly in the development phase and during use for various kinds of espionage, disinformation and value base manipulation purposes**. As a result, the understanding of a shared truth has been shaken, the experience of information security and data protection has disappeared, leding to escalating internal conflicts have. **Polarisation and tribalism** to which the *AI disasters* have contributed, have reduced democracies' and their decision-makers' ability to function.

The EU and democracies are being driven apart by outside aggravation of their internal and mutual conflicts. Populations within the EU have divided into tribes living around large corporations' technologies and those opposing techno-globalisation in their own ways across the political spectrum. Formulating common positions has become more difficult, weakening the EU as a regulatory body. While the EU's democratic institutions are formally up and running, in practice, the Member States use them to serve their national interests while playing their own games in the background.

Supply chains and EU infrastructure decentralise

Eroding relationships of trust have led to regionalisation of supply chains. Challenges in accessing minerals and technology in Western countries hamper the use of the devices and services that maintain the information society, and in terms of ensuring security of supply, leading to EU being at the mercy of those controlling large supply chains. Based on their economic and security interests and as a result of lobbying, the Member States are divided into camps that favour either American or Chinese solutions, **preventing the formulation of a uniform infrastructure policy**.

Large tech corporations in the United States market themselves in the EU as a safer alternative to Chinese solutions, offering themselves as strategic partners for public administrations. This results in **fragmented digitalisation development in the EU**, amidst in which Finland and Western European countries make their procurements from the United States or other Western countries or build joint solutions in their inner-state groups. In Eastern Europe, affordable and comprehensive Chinese end-to-end solutions are deployed in turn.

The Nordic countries as well as Western and Central Europe have stepped up their mutual cooperation. Mistrust in US and Chinese technology combined with the building of independent solutions slows down deployment, and **the different paces of technology deployment result in a patchwork infrastructure**. Eastern European countries are taking great strides, boosted by technology and infrastructure integrated in China's Digital Belt and Road cooperation. Due to worsening supply chain management, **cheap and insecure devices and obscure information networks** have become widespread.

Regulation cannot cope

The public administrations of a growing number of countries are 'collapsing' digitally as decision-makers cannot master the big picture of increasingly complex and unpredictable technology. Internal blocs hamper EU decision-making as the number of divisions has grown and the Member States have divided into smaller interest groups, paralysing the Commission. Finland seeks a primary reference group for its advocacy and reliable partners among the Nordic countries and in Western Europe. **In a volatile operating environment, regulatory efforts focus on the most acute security issues**, and protecting ordinary users from external threats and corporations' vagaries is overlooked. **Citizens' ability to enjoy basic digital security guaranteed by regulation is undermined as a consequence of numerous risks, and EU Member States can no longer reliably guarantee it for those with the lowest incomes.**

Large tech corporations take advantage of this opportunity to provide public administrations with key services as well as expertise in maintaining the tasks of the digital society and securing its continuity, expecting a less stringent interpretation of EU regulation in return. Consequently, the most useful functions in terms of collecting data from citizens and having an overview of supply chains are largely replaced with solutions closely monitored by these corporations.

Tax havens and free trade areas that are beyond the reach of international regulation are attractive locations for companies and cyber experts. They erode nation states' tax base and pools of experts, contributing to the reduced capacity of public cyber security bodies in democracies. They often also serve as platforms for cybercrime and subcontracting for APT actors that are difficult to hold to account.

Big Tech dependencies grow despite the mistrust.

Large tech corporations face greater opposition in democracies due to 'AI disasters' that partly resulted from the very tools the corporations brought out. In an unpredictable and volateile operating environment of the world economy, **however, their specialised subcontracting chains, maintenance resources and competence and their ecosystem identity management services are the only thing that can guarantee the continuity of digital societies.** The corporations strive to capitalise on their reputation as maintainers and quality assurers in the software world in the face of widespread 'loose cannon' AI-based coding solutions and deployment, which has inadvertently added to companies' technological debts. The building of common EU-wide applications and technological options faces political barriers, but the most determined Member States and groups are setting up their own solutions.

Big Tech companies compete for users, data, energy and markets. Having learned from the risks of national politicisation and the unpredictability of decision-making, large US corporations are circumventing the federal US state when building their profiles, striving to independently influence regulation and policy in their markets to create a favourable environment for themselves in democratic countries. **With state support, large Chinese corporations are strengthening their grip of Digital Belt and Road countries' infrastructures**, building efficient services for the digital societies while providing comprehensive solutions that enable large-scale user monitoring.

The growing sphere of influence of Chinese technology creates barriers to the spread of Western tech companies' solutions in the Global South, **the shrinking market area pushes Western companies to assume a larger role in democratic public administrations**, and under contracts concluded in a difficult economic situation, service providers often end up with more user data and access rights than is appropriate and actively use them to lock in the customer.

AI: Trust crumbles as a result of AI disasters

Agent AI applications have injudiciously been allowed to push their roots deep into democratic societies. Rapid launches motivated by higher productivity have centralised sensitive data to external service providers' systems, **giving external actors a detailed view of organisations' activities**. The accumulation of diverse sensitive personal and system data has made it possible for states and companies to spy on and manipulate platforms while allowing criminal threat actors to reverse engineer the accumulated sensitive data.

Political decisions have been justified with AI-generated information, and in addition to supporting decision-making, it has also been used to legitimise even unjust solutions. **Applications that contain unknown practices have been sold to public organisations and are being poisoned for geopolitical purposes.** Certain functions cannot be trusted because of such pollution, and attempts are made to restrict their use, but **some aspects of societies are no longer able to function without them, nor do they understand where such models are in use**.

The pace of AI adoption has slowed down. The threshold for allowing agent AI functions is now high, and there is a demand for defence against them. Threat actors are also actively acquiring the most advanced AI tools and agents. The sluggish development following the LLM boom has led to **computing overcapacity that is now for sale**. Criminals are setting up cryptocurrency companies to gain computing power for their operations under this guise. **With the data and computing capacity they have amassed, threat actors have been able to build advanced and specialised AI attack tools.**

Quantum-enabled trust?

Feverish efforts are made to build **trust solutions for the disrupted information environment** with quantum-resistant communication and encryption solutions. The most important forums of quantum research rely on affiliations between large corporations and the international university network. **Companies' quantum competence is a significant target for cyber espionage.** The major powers claim to have built decryption tools that give them access to all systems of the opposition, but in reality, both parties have ensured that their key systems are airtight and quantum resistant. **Because of internal dispersion and external influencing, not all EU countries have been able to switch to quantum-resistant protection. A significant backlog of hardware upgrades to run up-to-date PQC encryption algorithms has also hampered the development.** While rushing, there is a risk of using outdated standards with vulnerabilities. Critical infrastructure and defence applications are prioritised. The major powers focus on decrypting previously collected sensitive data to discover weak points for exerting influence.

Connectivity advances without a common direction

6G deployment is slowed down by dysfunctional supply chains, especially as use cases and demand are lagging behind. The standard diverges in two directions between Chinese and US companies. **EU suppliers have failed to bring their competing product to the market**, and the EU adopts the standard built by the United States. The effects of a multipolar and uncontrollable world are also seen in space as parties procuring space technology and satellite capacity diversify. Criminals operating through fronts acquire LEO capacity with the support of state actors **to operate outside other, monitorable networks**.

Decentralised supply chains have led to slower deployment of latest technologies in the EU and an uneven distribution of technology applications. **Actors dependent on services have varying visibility of where critical data is being processed, and they often have to take the service provider at its word for this. In the absence of a unified EU policy, building independent solutions is mainly only possible for the largest organisations and administrations.** For other actors, the best way to ensure continuity is to use the compatible systems of a single large service provider as extensively as possible, which leads to interoperability challenges at the EU level; the systems do not communicate well with each other, and there are vendor lock barriers to data portability.

When everything is synthetic, nothing can be trusted

Generative AI models that have been fed with information from the open Internet while recursively growing themselves and their synthetic output have resulted in **a self-perpetuating cycle, and the usability of the public Internet has crumbled as synthetic interaction has taken over**. This development breaks down the reliability of communication platforms, fragmenting citizens' realities into more separate, heavily moderated bubbles. **Different providers' platforms accessible to identified users offer different truths that shape users' world views**, and advertisers, synthetic agents and political information operators actively attempt to influence users on them. Personal AI assistants sold as neutral fact checkers integrate with media channels to analyse inputs.

Demands for stepping back from the digital information environment filled by 'digital pollution' have increased in Finland. Many people have been left behind or opted out of the digital transformation that advances in parallel with social inequalities. Some go on a digital fast, while many settle for a simple life with basic services. The 'organic use' of information networks with separate networks, interfaces protected against AI agents and local solutions are popular among hobbyists, and best practices are disseminated in communities. **The public administration is gathering its ranks to lay the foundation of trust and reach the 'lost/disappeared' citizens.**

On the Dark Web, platforms that have cleaned up their appearance and are easier to use have gained new popularity as **an escape from the public Internet for dissidents**. Their administrators are unknown, and the platforms are often unmoderated.

Destabilised information environment creates divisions

An uncontrollable world destabilises the security experience. A large volume of private data belonging to citizens who have accumulated a *personal data debt* in the 2020s has ended up in the wrong hands through various interfaces, and by combining that data, it has also become possible to target personalised scam and phishing messages at users who have kept completely out of social media**. A whole another story are the users who spent their time 24/7 with versatile personal AI assistants, disclosing biometric and detailed behavioural data**, based on which attackers can simulate complete, life-like fake avatars that interact as desired, for example for extortion purposes.

The society's foundation of truth has been destabilised, and citizens are mistrustful about disclosing their data to public administrations. The public Internet filled with synthetic content is not trustworthy, as interaction is marked by criminal agents and bots. Personal and organisational data leaked from smart systems and synthetic content created on their basis have been widely used to blackmail individuals and companies, court cases have become more numerous, and informed citizens have more negative attitudes towards disclosing their data. **Communities are introducing methods of poisoning and scamming sensors and smart features, such as *Nightshade* and *tar pits*, in order to escape companies' and authorities' algorithms.** The language used and the meme culture that continues to evolve rapidly have become an even stronger means of identification for breakaways escaping from algorithms when filtering synthetic content in the *Dark Forest* of the public Internet.

While ethical and transparent data processing is becoming a competitive advantage, the change is happening slowly, and building trust is difficult. The **reintegration** of breakaway citizens from digital society **while allowing them to opt out from digital systems** is emerging as a dilemma in Western countries.

Attack surface: Patchworks of systems

- Large service providers are particular about who is allowed to connect to their clouds, as AI agents mapping IT and OT vulnerabilities have drilled through the supply chains. Users and companies able to pay have to go through a 'detox' process as their own systems coded with AI assistance have often proven insecure, forcing them to renew their digital identities and systems in order to connect to quality-controlled Big Tech ecosystems.
- User data are stored in a less centralised environment and unknown locations where they are handled by outdated and vulnerable IoT and edge devices. More local implementations have been put on the agenda, but are difficult to justify from the business perspective. Finns mainly focus on network segmentation.
- Service providers careful about their system integrity offer secure comprehensive solutions for wealthier operators with a higher maturity level, and SMEs are left on their own in terms of high-quality information security.
- Citizens are using a wide variety of applications containing obscure practices, which may include data loggers concealed with pseudo-features, such as bots that fact check news streams. Communities' trusted local networks are protected by methods that aim to block and deceive agents.
- More private digital ecosystems have emerged on the Internet and Dark Web which, together with free trade areas, enable 'virtual states' where criminal cryptocurrency is laundered through operators disguised as legitimate institutions. No common ground for supervising and sanctioning such safe havens for crime can be found, as they may be fielded as geopolitical proxies.
- Security problems emerging in AI systems have reduced trust in autonomous cyber defence applications, while the capabilities built by attackers with specialised AI attack tools are having a field day.
- Continuity management has become more complex due to unknown nodes, whereas fragmentation at the same time hampers malicious activities; the use of technical descriptions based on different systems and standards, some of which are outdated, is laborious, and even an AI-assisted attacker cannot find training data to cover every detail of legacy systems.

Threats: Fragmentation creates unpredictability

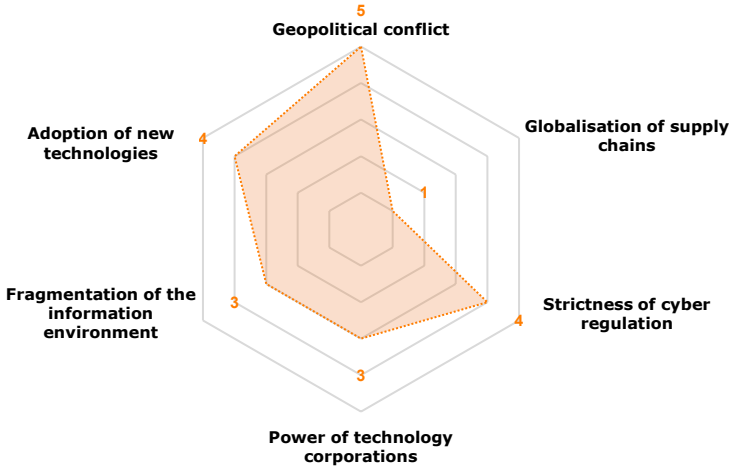
- State-backed professional criminals operating in the new virtual states and in countries with crumbling regulation have acquired an unprecedented level of compute capacity and use effective AI tools for attacks, analysis and combining data.
- State actors and criminals influence satellite constellations by cyberattacks, and incidents and disruptions in satellite functions are more frequent. Mobile phone networks, power grid management and transport systems suffer from synchronisation errors and falsification of time and geospatial data.
- Combinations of interaction data from dating services, Internet browsing data, LLM access data, health application biometrics and bank data as well as large-scale leaks enable criminals to perpetrate highly profiled deepfake scams, including ones appealing to emotions.
- Threat actors harness code agents to instantaneously create genuine-looking copies of trusted applications and platforms to trap unsuspecting users.
- The cutting-edge cyber capabilities of both parties honed during Russia's war of aggression in Europe in the 2020s are for sale in the global market.
- *AI zero-day vulnerabilities* occur when vulnerabilities that are triggered under certain conditions are hidden in models' memory, training data or context, for example by manipulating an AI application's long-term memory.
- Work platforms disguised as legitimate by state actors and criminal groups in virtual states provide an additional source of income for professionals. They are used in attempts to recruit local insiders from IT companies that have taken precautions against deepfakes.
- Ineffective control of sanctions in the EU's fragmented regulatory environment has led to an increase in ransomware trojans exploited by criminals, as there are no trade policy barriers to paying ransoms, and companies primarily seek to maintain their good reputation. SMEs are affected by thisin particular.
- In the aftermath of the AI disaster, an increasing number of systems are protected by *'tar pit'* countermeasures that slow down AI agents and give them the runaround, but criminals are also developing methods for corrupting the operation of scrapers and AI agents used by organisations to trap attackers.


/TWO REALMS/

/TWO REALMS 2035/

Geopolitical confrontation brings the world to the brink.

The Western bloc led by the United States faces a challenge to world order from China and its allies. There are efforts to destabilise the joint Western front by testing the NATO countries in Europe. Gaps are sought in their critical infrastructure, and a calculated approach is taken to NATO intervention. **The EU has responded to emerging threats by building digital lines of defence in cooperation with the United States, with almost complete dependence on its technologies and the NATO.**



Tech giants toe the line.

Subordinate to their countries' public administrations, tech giants **participate** in the major powers' geopolitical strategies in such areas as data management, AI development and security infrastructure. The geopolitical benefits of tech giants have grown, and they influence governments in order to expand. Defence administrations in large NATO countries have their **representatives within technology companies**. Their **platforms serve as tools for and targets of intelligence collection**. Tech giants actively support the growing influence of their blocs, including through backdoors and espionage technologies, hoping to secure access to critical factors of production in return. **Analytics companies of the US defence sector have integrated with EU countries' administrations.**

Technology is taking great strides in AI defence systems.

Autonomous cybersecurity AI applications have become a critical part of societies' security architectures in the race between the major powers, as **autonomous attacks have significantly reduced the response time available for defenders, creating a continuous race between code agents developed for attack and defence. Functions critical for security of supply**, from food supply to water service infrastructure, **have been handed over for AI systems to manage**. However, there is still an effort to keep humans involved in decision-making as tensions heighten in the security environment. 6G and satellite broadband have ensured that connections within the geopolitical blocs are delay free and high in capacity. **As the major powers' AI solutions are closely matched, quantum technology is being developed towards military applications.** The threat of quantum supremacy has made quantum-resilient algorithms the key project of development, and both blocs have managed to protect the most critical data resources with them.

External information influencing is restrained.

Communication channels and platforms in the blocs are controlled on ideological grounds. The Internet preserves its apparent freedom, whereas in practice, it presents a virtually and ideologically controlled and filtered regional reality. Synthetic media and deepfake technologies are actively used to safeguard and attack against the information environment. **Platforms are increasingly administrated by state actors, and authorities filter, prioritise and edit information.** The efforts to censor external spreaders of disinformation also extend to internal dissidents. **The EU's role in data protection is unclear in relation to platform administrators, but this is accepted as a necessary sacrifice to maintain external and internal security.**

The spheres of interest isolate their supply chains.

The United States strives to build independent technological supply chains to continue advanced chip production, facing vicarious conflicts in Africa, South America and the Caucasus. **Western countries' competitiveness has been reduced by goods flows affected by trade policy divergence, demographic challenges and availability disruptions resulting from regional conflicts**, while China's technological dominance in the fields of AI, automation and data infrastructure has put them on the back foot. Global digital infrastructure has split in two. **The EU's bid for sovereignty has remained ineffective**, and US hyperscalers' infrastructure dominates in critical information systems. **EU cloud environments are also built on and monitored by them.**

Political securitization tightens regulation.

Technological interoperability and standards between the blocs have declined, and basic infrastructure is based on systems tied to the geopolitical bloc. The United States demands that its digital infrastructure companies be allowed to operate and carry out monitoring as freely as possible in the EU, justifying this by their status as *the critical infrastructure of the West*. There is a sharper focus on security in EU regulation, but security slips through the EU's hands as **representatives of the United States coordinate digital structures with the authorities**. As control increases, right to data protection is breaking down. Monitoring tasks have been handed to large service providers, including AI-enabled facial recognition.

Geopolitical confrontation brings the world to the brink

The US-led western bloc is trying to prevent the spreading influence of the alternative technological order represented by China and its allies in world trade, global standardisation and regionally. China is using its central position in the economy and politics to take its place as a **guarantor** of common institutions and **new rules**.

The NATO countries are being tested in Europe by means of 'special operations', which include cyber and hybrid operations, information influencing and the use of energy as a weapon to destabilise the Western bloc. Vulnerabilities are sought in critical infrastructure, and a calculated approach is taken to NATO intervention.

The United States, where democracy is declining, has attempted to expand its influence by force on the Western hemisphere and to boost intelligence collection throughout the world through US-based technology companies. While struggling with its national conflicts and internal challenges, the United States strives to build supply chains independent of China to support the defence industry, chip production and technological spearhead industries. However, it faces vicarious conflicts in South America, Africa and the Caucasus. The EU has responded to the geopolitical struggle by building digital lines of defence in cooperation with the United States and NATO. The EU is completely dependent on their intelligence and the systems offered by US companies, having lost its sovereignty in exchange for its security.

The spheres of interest isolate their supply chains

In relation to China's more self-sufficient authoritarian bloc, the Western countries' competitiveness has been eroded by geopolitically diverged goods flows, demographic challenges and supply disruptions resulting from conflicts, and the global infrastructure has been divided in two. Chip production has found new channels following disruptions in the production capacity in East Asia, which has reduced the AI competitiveness of the Western countries in particular. China's technological dominance in the field of AI, automation and data infrastructure has put the Western countries on the back foot as they lag behind in productivity, forcing them to protect their innovation potential while a **growing number of states collaborating with China are rapidly adopting affordable and scalable stack technologies, such as AI surveillance tools**.

The EU's bid for digital sovereignty has remained ineffective as the Western countries' economic room for manoeuvre has shrunk. **US hyperscale companies' infrastructure dominates strongly in critical information systems. EU cloud environments also rely on these companies for their defence**, while the cooperation is conditional on keeping away from Chinese solutions and technology. **Technological interoperability and standards between the blocs have declined**, and even basic infrastructure – such as satellite networks and 6G data transfer – is based on systems tied to the bloc.

Political securitization tightens regulation

With significant technological strides forward, China has become the leading standard-setter for new technologies. The United States has demanded favourable regulation and treatment for its large service providers in exchange for securing the EU's digital infrastructure against the authoritarian bloc. Representatives of United States companies and authorities coordinate the management of digital structures with EU authorities in order to maintain a strategic overview. Hyperscalers have developed efficient autonomous AI applications in which certified service measures and maintenance of critical applications are a precondition for security in the tense geopolitical situation, as well as increased monitoring of digital infrastructure in general. Stricter requirements have been imposed on the traceability of activities, and control of the use and development of permitted applications and facial recognition alike have been handed over to large service providers.

Increasing control makes individuals' and companies' activities more transparent to public organisations and intelligence services observing them. The GDPR has in practice been repealed in the EU, and the Data Protection Ombudsman's role is significantly narrower. Intelligence authorities' AI applications analyse activities to identify deviations, improving national security while also ending up on a collision course with privacy and legal protection, as this leads to wrongful convictions at times. The right to data protection is at breaking point, and interpretations of the individual's information security rights vary from state to state.

International data regulation is fragmented, and the level of regulation applicable to large corporations varies globally and between the blocs. **While regulatory authorities take on a more significant role, practical implementation is a struggle and influenced by strong lobbying.** The EU's cybersecurity role is enhanced as the NIS2 Directive/Cybersecurity Act gives EU institutions added power and responsibility for coordination. **Dedicated security authorities are set up for digital infrastructure.**

Tech giants toe the line

Technology giants are forced to operate more obviously as part of the major power policy, placing themselves in the sphere of influence of either the United States or China. They are actively involved in geopolitical strategies – such as data management, AI development and security infrastructure. Defence administrations in large NATO countries have their permanent representatives within technology companies. **Companies are used to spread states' influence, and their platforms are both tools of and targets for intelligence.** Analytics companies in the US defence sector have integrated with EU countries' defence administrations through their AI capabilities. The geopolitical benefits of tech giants have increased, and they **influence governments in order to expand and deepen their market positions**.

Tech giants actively support the growing influence of their blocs, including through backdoors and offer of espionage technologies, hoping to secure access to critical factors of production, such as minerals, in return. Large US corporations seek to expand the Western sphere of influence by building supply chains and digital infrastructure in friendly countries balancing between the blocs, acquiring leverage where necessary in the form of export bans on key technologies, political influencing and supporting limited use of military force and economic weapons.

Strict EU regulation has not opened doors to large corporations' boardrooms, and EU pays the price for dependencies. The geopolitical situation hampers free innovation and decentralisation of investments, accumulating expertise to large American corporations, for which the United States **demands the right to operate as freely as possible**, justifying this by their status as the *critical infrastructure of the free West*.

Autonomous attacks and defence are growing more frequent

AI has taken on a critical role in of societies' security architecture in the technology race, as **autonomous attacks by state actors and criminal networks have shortened the response time available for defenders, creating a continuous algorithmic race**. Autonomous AI models are built for attack purposes with specialised datasets, and in response AI systems monitor infrastructures and services in real time, for which large service providers' coding and patching agents need access to critical EU systems. **Along with the reorganisation of value chains and technological leaps, Chinese and US solutions are equally matched.**

AI agents handle data analysis and risk management and support decision-making in both private and public organisations. *Cyber twins*, which are simulated to produce proactive analytics for preventing and blocking data leaks, are used in real-time modelling of virtual defence systems. Decentralising data and restricting administrators and access continue to be key adaptation mechanisms.

The use of natural language AI applications and agents has become commonplace in coding, which results in their control becoming a problem. The largest organisations (incl. defence administrations) uphold **moral, ideological and legal programming** in AI agent ecosystems, and by observing these principles, agents can be calibrated to act transparently towards the authorities while they are also vaccinated against external influence and programming attempts.

The quantum race is the next strategic spearhead

Quantum technology has moved on from the experimental stage to a strategic resource which, as the major powers' AI solutions are equally matched, is being developed for military applications. As a result of the threat of quantum supremacy, developing quantum-safe algorithms has become the key defence project in the West, and the most critical data pools have been protected with encryption algorithms stronger than cryptography. Mistrust is seen within the blocs, as examples of military and intelligence use of breakthroughs, even to spy on allies' data, have come to light.

New risks emerge in connected defence infrastructure

The world has moved on to an era in which connections inside the geopolitical blocs with diverged standards are almost delay-free and have a high capacity through 6G, software-controlled networks and satellite broadband. **However, information no longer moves freely as technological structures between the United States, China and the EU have diverged.** For defence purposes, the EU's IRIS^2 satellite capacity is complemented with US service providers' satellites where **built-in dual-use technologies are actively employed to enable efficient monitoring within the region and externally.** The EU depends on US companies for its satellite operations.

Society's digital dependency has grown, and the functions critical to security of supply are increasingly being managed by AI systems to counteract the response time shortened by autonomous attacks. As computing-intensive and AI-assisted digital defence infrastructure and energy-intensive data centres maintaining it are built, the **energy system is the most critical node in society**.

The increasing number of network edge devices are a critical and growing problem, as attacks on their data that handle sensitive information on society's attack surface are continuous. **Platform agnostic solutions are used for added flexibility and to reduce locking in to certain critical systems**, and they are tweaked in the Western countries for use in flexible transfers of data and functions between service providers. **Satellite connections have become a key threat vector because they serve as backup capacity in case of disruptions in physical connections caused by sabotage.**

External influencing by information is restrained by force

Digital communication channels and platforms are under the strong ideological control of the major power blocs, and the Internet is no longer genuinely global for users. While **the Internet experienced by citizens preserves its apparent freedom**, in practice, it shows a carefully guided, **filtered reality**. AI assistants gradually rewrite history in the geopolitical blocs, and information that is incompatible with ideology disappears.

AI, synthetic media and deepfake technologies are used to both safeguard and attack against the information environment. **Platforms with big user data and personalisation data** defend against geopolitical waves of propaganda with **active censoring by AI assistants**. **Micro-targeting is used to disseminate a world view and content that upholds 'Western identity'.**

Management of information environments by state actors increases, and authorities use filtering, prioritisation and editing. In education, the focus is on teaching information literacy. Better preparedness and protection of data are required of companies also in the information dimension. Misleading communities and influencing networks are identified, and their visibility is actively restricted. **Efforts to censor external spreaders of disinformation extend to internal dissidents, and the truth is often blurred in the name of national security.**

The EU's role and impact in managing the information environment is unclear in relation to platform administrators, as all information flows to US intelligence through large corporations and specialised security sector analytics companies. This is accepted as a necessary sacrifice to maintain the EU's external and internal security.

More monitoring and mounting resistance

Breaking away from Chinese supply chains has raised consumer prices significantly in Western countries. While defence expenditure takes its toll, social inequalities erode national cohesion in EU countries, and citizens' daily digital life is increasingly directed based on security perspectives. The list of approved applications and devices is limited, and only EU-validated US solutions are allowed in Western countries. **User interface functionalities are restricted to prevent misuse**, and personal AI systems monitor users' activities to detect deviations. Skin contact identification (incl. smart textiles, wearables) evolves as a security and identification solution.

Security becomes a lifestyle for some and fuel for rebellion for others. AI-based monitoring systems are used to recognise external sources of disinformation and to identify internal threats within the bloc. Well-informed users attempt to access freer information against payment through different routes, but an indifferent majority adopts the safe, filtered world view. Critical citizens seek to circumvent the restrictions by going to informal, foreign platforms in search of alternative news. Consequently, user groups can unknowingly end up on **targeted foreign platforms that look western but collect and pass on information for geopolitical state actors**.

Attack surface: Cyber-physical systems under AI monitoring

- The boundaries between cyber defence and offence have practically disappeared, and in the cyber dimension marked by heightening geopolitical tensions, AI agents battle each other, attempting to influence each other's programming and training data.
- The Western countries have barricaded society's critical, connected systems behind quantum-safe digital walls with AI-assisted monitoring maintained by large tech corporations.
- With AI-assisted, real-time shock-resistance, society's digital security finds its concrete expression in defence AI infrastructure, such as electricity, data centre, satellite and cable configurations. Human-controlled *virtual SOCs* run by defence agents and AI systems are becoming more common.
- Growing connectivity covers areas of society from digital border control to factory OT systems. In the context of hardened software and hardware systems, the need arises in particular to address risks arising from users, social engineering and insider activities.
- AI-assisted monitoring by specialised US analytics companies is targeted at user activity to discover deviations and identify internal threats. Information security companies also have a duty to disclose information about users' suspicious activities.
- User monitoring is carried out with built-in backdoor software in approved smart devices that are regarded as secure. These devices are used to access basic digital services as well as tools such as personal AI assistants.
- Users' obligation to keep their devices up to date is highlighted, and more education relating to this is provided. Permitted activities and devices are subject to significant restrictions, which may go unnoticed by the user due to censorship.
- Screening based on extensive analytics and behavioural data to identify employees suited for different levels is used in IT companies' recruitment. A single mistake in social media history, a bias in the selection algorithm or false content created about a person can be a barrier to employment that is identified by combining data.

Threats: State actors target critical infrastructure

- The nodes of digital and cyber twins that manage the systems controlled by *security AI's* are targeted by state actors' cyber and hybrid influencing, through which attackers attempt to eliminate the level of autonomous cyber defence. After spying on a system, influencing can be targeted at an individual agent, which in turn leads to a snowball effect through downstream replication in other agents. Manipulation of defence applications' training data is also part of the toolkit. Human-in-the-loop models do not scale sufficiently, exacerbating unpredictability.
- Because of their AI interfaces, the smart grid OT systems and edge devices of energy systems that maintain societies' cyber defence are prone to backdoor risks.
- Historical, sensitive user data disclosed by breaking quantum cryptography are used to blackmail and manipulate people working within critical security systems in Western countries for espionage and sabotage purposes.
- Under the guise of society's increased control and manipulation of information, hactivists whose strings are pulled by authoritarian states strive to radicalise anti-West shadow societies which can be mobilised to act against physical infrastructures and used for identifying insiders in critical infrastructure companies.
- Espionage is targeted at satellite and space programmes, and there are active efforts to sabotage them through cyber methods between the blocs.
- In the geopolitical blocs' offensives, state actors' AI agents programmed to carry out autonomous vulnerability mapping and build suitable malware for attack purposes can be launched without sufficient control, leading to significant collateral damage and also their spread in the attacker's own supply chains.
- APT actors are striving to poison autonomous combat drones, which were rapidly developed in vicarious conflicts between the geopolitical spheres of interest and which are used in autonomous border control and police activities in the EU.
- Due to critical function connectivity, even automated agricultural components ranging from autonomous farm equipment to greenhouses are channels through which APT actors attempt to destabilise societies and the security of supply.

TRAFICOM

/DATA EMPIRES 2035/

No limits to advancement and connectivity.

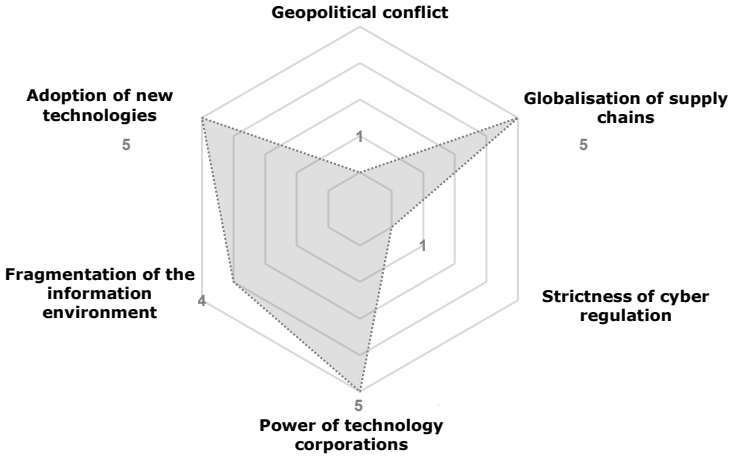
AI models have become widespread due to the availability and mobility of diverse data. The data empires maintaining the Mind² environments built around them manage user data globally and know more about individuals than public administrations or the users themselves. A significant part of the world's population enjoys the comforts of smart homes connected to AI systems, and **wearables are as common as smartphones**. US companies are at the forefront of quantum technology development. **Companies and organisations have extensively introduced quantum-resilient encryption as data empires have set up PQC algorithms in their systems.** Space technology is a competitive arena due to the increasing importance of intelligence, strategic armament and satellite services.

Personalised halls of mirrors.

Users are attracted to large service providers' **sensor- and AI-based, real-time Mind² environments** that offer a holistic digital lifestyle. The data empires compete by locking in users to their environments. Disclosure of biometric data for monitoring is a common gateway to cheaper, better and more targeted services. **Experienced realities diverge based on income levels and the service ecosystems used.** The data empires' platforms enable personal AI assistants and on-demand application development for people while **shaping the behaviour of users interacting with them in keeping with advertisers' and administrators' goals.** The spread of natural language AI interfaces and synthetic communication stunts people's ability for critical thinking.

Big Tech strives for independence from nation states.

Tech giants are spreading their monopolies and tentacles. With their help, the United States has established its position as a hub of technology and standards, whereas **political influence has shifted to the data empires' boardrooms**. China is about to overtake the US with its technological advances, ownership of resources, production and sphere of influence. Bolstered by AI development, data empires use their position as administrators of the largest global interaction platforms to **influence elections and politics around the world** in order to build a favourable operating environment for growth and resources for themselves. The EU's role is that of the data empires' customer, and it is seeking to stabilise its geopolitical relationships in hopes of growth.



Few can master the technological complexity.

The largest US tech corporations have cemented their position in the Western countries. They manage to avoid regulation by making themselves irreplaceable. They copy competing applications to their portfolios using efficient coding agents or buy them out and bury them, **making it extremely difficult for EU companies to bring their solutions to the market**. Supported by Digital Belt and Road infrastructure diplomacy, large Chinese corporations have spread their influence, and the vast majority of people in the world are influenced by their infrastructure, which centralises monitoring and behavioural data.

Growth at all costs.

Technological innovations making headway in a stable operating environment of the world economy have brought on desired growth, albeit unevenly distributed, **while their maintenance requires increasing amounts of environment-burdening resources**. **Data empires manage to mitigate protectionism in order to maintain stable value chains essential for growth** and to preserve their access to world trade strongly dependent on China. Russia is reintegrated into the world economy in order to guarantee affordable energy. **Technological subcontracting chains operating around US and Chinese companies**, which these companies alone can manage, **are the lifeline of national economies.** All countries, including the EU, are divided into companies' 'spheres of interest' based on their main customer accounts.

The rising level of abstraction hampers regulation.

Regulation cannot keep up with large corporations' technological development. Public administrations are increasingly incapable of managing ever more complex digital environments, and data empires capitalise on their positions, getting their representatives into key national and EU decision-making bodies. **Parliamentary decision-making is increasingly dictated by the AI tools made available to public administrations by data empires.** Service providers take care of protecting the data of the customers who can pay for it, and those in the lowest income bracket are less able to enjoy a basic level of information security regulation. **The EU has grown weaker as a political actor and regulator,** but cooperation between the authorities has stepped up to protect ordinary citizens from cybercrime in areas in which the data empires have no interest.

Big Tech strives for independence from nation states

Tech giants are spreading their monopolies and influence around the world, supported especially by successful AI development at scale. With their help, the United States has maintained its position as a hub of technology and standards. However, China's technological advances and ownership of resources and production have increased, its applications dominate the world, and its sphere of influence is growing through alliances. **The data empires succeed in reducing the confrontation between the US and China in order to maintain stable value chains** and world trade dependent on China in order to sustain growth. As a trade-off, political influence in the Western countries has largely shifted from democratically elected decision-makers to ***data empires'*** boardrooms, where politicians exchange public administration resources, favourable regulation and international influence for status and election funding.

Technological innovations making headway in the relatively stable operating environment of the world economy have brought on desired growth, albeit unevenly distributed, while their maintenance requires increasing amounts of resources that burden the environment. **Data empires seek ways to exploit US foreign policy to build a favourable operating environment for themselves, seeking opportunities and resources for growth primarily through opinion campaigns and, if necessary, through regional use of force.** Bolstered by AI development, they use their position as administrators of the largest global interaction platforms to break states away from market-disrupting nationalism while influencing elections and politics around the world.

The EU has updated regulation adopted in the 2020s for the 2030s and requires **higher security standards of companies** operating in the region than what the United States is prepared to accept. The data empires protest against this, threatening to restrict the availability of key applications, and the **EU is forced to bow to demands of relaxing AI regulation, among other things.** Economic interests and concern over the continent's competitiveness are driving a wedge between the Member States, causing their interests to diverge dramatically and eroding their capacity to make joint decisions.

Growth at all costs

The EU is not capable of forging a uniform infrastructure policy while large Chinese and American corporations are dividing the market into their 'spheres of influence'. US services and supply chains are still remembered as unreliable by some EU states, due to their repeated use for geopolitical leverage in the 2020s. China is taking advantage of this opportunity to offer Western countries more advanced technology to replace its American counterparts.

Data empires are constantly grabbing more data, computing power and the latest chips, ensuring that their prices and the latest applications are out of reach for smaller operators. The empires have used the data collected in real-time to monopolise software development through their AI code agents. The EU decides to sit on the fence between the major powers' service providers, **seeking the best solutions in the US and Chinese markets alike and choosing the middle road between pragmatism and security considerations.**

The EU is lagging behind in development and does not want to lock itself out of any networks while it is seeking growth opportunities offered by technological development. **In practice, the EU's most critical cloud infrastructure is still European or American but consumers, for instance, use a large volume of Chinese infrastructure and applications.**

Few can master the technological complexity

The data empires rely on continuous growth as well as the complex supply chains, resources and need to centralise energy required by the latest technological solutions for their power and prosperity. As a result of the AI development, societies' service provision is centralised based on the scaling benefits offered by the empires' data infrastructures. There are subcontracting chains operating around large US and Chinese corporations, and the large corporations alone have an overview of them and can control them, and in practice, serve as the lifeline for the national economies who are the empires' customers.

In particular, companies that have built US AI services have succeeded in cementing their influence on consumers' and legislators' activities and decision-making in all Western countries. They manage to prevent regulatory efforts by staying at the forefront of technological development, spreading their influence in societies and making themselves irreplaceable. AI-assisted advances in coding automation have further centralised influence in the hands of the largest hyperscalers. From the user's point of view, the weaker competitive setting has significantly stunted a number of services, which is why new competitors are actively seeking to challenge the data empires' monopolies. **However, innovations are targeted by direct espionage for development carried out on the data empires' platforms**; the empires use potential competitors' technologies in their own portfolios or buy out and silence them to protect the position of their own solutions. This makes it difficult for EU companies to get their solutions to the market. **Data residency is in large corporations' parent countries.**

Large Chinese corporations have spread their influence especially in the countries of the Global South with the support of Digital Belt and Road infrastructure diplomacy. The majority of people in the world are directly influenced by their applications and infrastructure used for monitoring and centralisation of behavioural data. With the support of the Chinese government, they are preventing Western companies from encroaching on their sphere of influence while also striving to take over a market share in democracies by framing their services for the state and society as an alternative to *private monitoring capitalism* in the West that enables *dignified life*.

The rising level of abstraction hampers regulation

Regulation cannot keep up with large corporations' technological development, and the aspiration of **digitalising and enhancing the efficiency of societies as an end to itself overshadows fulfilling the nation state's duties**. Increasing amounts of public administrations are incapable of managing the increasingly complex digital environments, and the data empires are starting to exploit a regulatory vacuum, **striving to get their representatives or employees elected to the national and EU decision-making bodies** that are the most important to them. **When they feel that regulation threatens their power and business, they engage in effective opinion campaigns and lobbying** to get their way. Parliamentary decision-making and its justifications are increasingly dictated by the empires' AI tools; AI outputs are equalled with expert knowledge, and fewer consultations are conducted.

The EU has lost momentum as a political actor, but cooperation between authorities has been stepped up in operative activities to safeguard citizens from cybercrime. **Service providers take care of protecting the data of the customers who can pay for it, and those in the lowest income bracket are less able to enjoy a basic level of information security regulation.**

AI scaling is prioritised when the new technocracy builds its fences

AI models have become widespread in global information networks due to the availability and mobility of diverse data. Their administrators manage user data globally and know more about individuals than public administrations or the users themselves. **Decision-making in democracies has been covertly taken over by algorithmic steering through administrations' new user interfaces.** AI systems usually contain backdoors for data empires, or they cannot be audited by the authorities. As autonomous technology moves to black boxes, this **makes it more difficult to assess the ultimate purposes of applications and agents as well as the issues of responsibility, security and privacy associated with them**. Through major powers' demands or in cooperation with local governments, the platforms may also block content, manipulate opinions or exert economic pressure in a specific region.

The vendor lock-in phenomenon has gathered momentum **as large corporations' own code agents drill down into organisations' supply chains to build systems that are only compatible with specific organisation's stacks. Data empires block each other's agents by restricting their rights and only build interfaces with their partners.** Programming is centralised in the hands of hyperscalers, as autonomous code agents weld together components between systems and optimise activities in real time, for example in cyber-physical environments. Through self-learning, this arrangement enables agile re-routing of supply chains in fault situations. **The result of code agent introduction is widespread unemployment without coordinated public programmes for managing its consequences, and the trend of increasing inequalities speeds up.**

Going for quantum innovations

As AI systems have established their position in societies, quantum computing, which is more energy-efficient than semiconductor solutions, attracts the data empires' interest, which attempt to **combine quantum algorithms with machine learning programmes**. Quantum computing in QCaaS services has created significant benefits in the pharmaceutical and logistics sectors. **US corporations have made it to the forefront of development by adding EU companies' capabilities to their portfolios, while Chinese companies are hot on their heels.** Organisations have switched to quantum-resilient encryption with the introduction of data empires' PQC algorithms.

Unlimited growth and connectivity require resources

The largest AI applications have initially been tripped up by the depletion of public training data. **As a solution for the next step, the data empires' diverse services are bundled into a single user interface, 'collective brain', (*Mind*²), to which users connect with wearables and biometric chips.** The user interface collects data on interactions and vital functions for training needs through AI agents, creating 'collective', real-time understanding between users. **A significant part of the world's population enjoys the comforts of smart homes, and wearables are as common as smartphones.** The 6G network links satellites, drones, terrestrial base stations and IoT devices into a seamless system. Network control is based on AI and ML that optimises resources in real time. **AR, VR and metaverse environments operate without delay.**

The data empires' 'collective brains' and their protrusions are built on huge physical-world infrastructures, resulting in constant demand for more energy and components. Growth is sought indifferent to the form of energy, heedless of climate and environmental factors. **Space technology is a significant arena for corporate competition** due to the increasing importance of intelligence, strategic armament and satellite services. **Computing capacity is taken to the orbit with data centre satellites** as panel technology development ensures a better energy supply for satellites. The data empires need minerals for their growth, and **asteroid mining technology is being developed to guarantee raw material streams**.

The well-off can escape a world of manipulation

A price has been paid for rapid AI development and connecting synthetic content producers to platforms, and the public Internet has been filled with difficult to control digital pollution. As a result, **users have turned to large service providers' *Mind² super application environments* where quality is controlled by AI assistants and AI curation**. These environments provide people with experiences of effective and secure digital existence as well as peer-verified information sources in different price categories. Thinking is shaped through the 'collective brain' and by its impact, and the individual's ability to pay determines their access to the best understanding.

A somewhat uniform understanding of the world is left behind in the 2020s. The data empires have later fenced private and public data and users in comprehensive information environments that only the empires can access. Experienced realities **diverge based on income levels and AI ecosystems used**. Premium-level users pay to shape information environments according to their wishes, standing out as the elite. **Companies strive particularly for the appreciation of these 'high-value users', whose information security is looked after.** The 'middle class of data' go for a holistic lifestyle with metaverses based on individual and personalised algorithm control by an assistant. Those who have opted out of AI environments favour individual pay wall media or seek the *'truth'* on the Dark Web and other alternative environments. As constantly adapting natural language and human synthetic communication become more common, **ability for critical thinking is stunted, making the ideas fed to people more powerful**.

Small state blocs are able to verify reliable information internally, **but in the big picture, information management is no longer possible due to the fact that the data empires have largely fenced in the digital commons**. State governments focus on information that can be confirmed as a fact in the real world.

Personalised halls of mirrors

Data empires lock in as many users as possible to their platforms and environments to collect more and more data concerning them and to guide their behaviour. Technology becomes a way of life similar to religion, in which life guided by algorithms is a desirable state. **There are continuous interfaces from AI assistants to sensors that are used for data disclosure.** Companies are rapidly developing LBM (*large behaviour model*) solutions based on wearable sensors. Sensors and devices are linked to super application environments with different payment levels to improve the personalisation of services. The disclosure of biometric data for monitoring is a common gateway to cheaper, better and more targeted services that can be instantly generated through the data empires' application store and personal assistant agents.

Freemium users disclose their data for services and are targets for advertising and bot influencing. **Free versions of AI assistants serve as personal companions, shaping consumer behaviour** in line with advertisers' goals. Applications generated by free users include deeply personalised advertisements. As a consequence of manipulation, users start to reproduce machine intelligence features, whereas higher fee categories include highlighting unique features, experiences of humanity and better tailoring of self-generated applications.

Data empires isolate people from their nation states and other communities, transferring the most productive parts of users' cognition to the empires' interfaces and user interfaces. The Dark Web and alternative communities are actively used as escapes from full visibility in the digital world. The smoothed-out digital life and its interfaces are in sharp contrast with the **physical worlds' extreme weather phenomena, increasing displacement, inequalities and an environment increasingly burdened by local resource conflicts.**

Attack surface: Overheated connectivity

- Data empires work as the key security providers are concentrating significant resources to protecting the most important data resources of their Mind² configurations. They also accumulate best security practices and identified vulnerabilities as their trade secrets. While agentic AI vulnerability detection and patching gives tech giants better ways of deflecting traditional attacks, they have little motivation to protect anyone other than their premium users and systems.
- Advancing connectivity has provided cyber criminals with more opportunities to extend their impact to an intimate level of users' lives. Everyday functionality supplemented with devices depends on a wide range of interfaces and devices connected to the individual's person, exacerbating vulnerabilities.
- Large-scale AI integration into core business functions has centralised sensitive data in organisations to specialised systems, turning them into attractive targets. Citizens are being profiled in the life interfaces more accurately, and privacy protection can be acquired as a luxury product. SMEs have trouble protecting their data because secure data processing has become expensive.
- In the cyber dimension, state actors focus on eradicating cybercrime in international cooperation and on bringing cybersecurity to areas where data empires' activities do not extend. APT operators focus on phishing and industrial espionage for the benefit of the parent state's business operations.
- Regulation that cannot keep up with technological development has watered down the right to data protection and data security for those left outside the empires' ecosystems. Cybercriminals extend their activities to areas where the empires have no economic motivation or regulatory obligation to spread their safety nets.
- Companies accuse states of politicising technology and emphasise that they protect their users, obscuring visibility to their actions.
- As a result of connectivity, the reference point for all programming and code is provided by the data empires' constantly updated, real-time big data, based on which AI agents build systems autonomously. Historical information, old websites and content as well as best practices are at risk of being lost.

Threats: AI datafication leads to new forms of crime

- Various subcontractors in the data empires' supply chains are the primary targets of cybercriminals seeking to steal the personalisation data they collect.
- Micro-targeted fake versions created with code agents that imitate Mind² user interfaces and services are rolled out by criminals to steal user data. As sensors and the attack surface cover the digital lifestyle from widespread home robots to AI assistants and biometric chips, data combination enables the creation of fully credible virtual copies of people on official platforms for a wide range of criminal purposes.
- Example: the lifestyle user interfaces that have become common in Mind² environments have accumulated information on premium users' behaviour and spatial data, and database breaches enable personalised cyberattacks. Data are then sold on the Dark Web. Premium user accounts are also cloned in an attempt to get close to data empires' other wealthy users for scamming purposes.
- Attackers can even break data empires' security arrangements by using surprising attack vectors, including outdated data and zero-day vulnerabilities that self-learning systems have not seen in their training data. An injection attack based on old software libraries can target code agents through supply chain legacy systems, causing the entire supply chain to crash.
- Platform companies' advanced protection mechanisms, moderation of the information environment and increasing costs of successful attacks have led to the disappearance of impactful and visible hactivism. Attacks against infrastructure by activists and religious parties opposing the AI lifestyle take the form of physical sabotage. Infrastructure is also attacked by activists whom the building of computing power has exposed to *resource imperialism* in geographical crisis areas. This results in an unexpected paralysis of critical services of society.
- The impact of AI is seen as increasing redundancies in the IT sector, which has significantly grown the insider risk. On the Dark Web, active attempts are made to recruit data empires' ex-employees to criminal organisations as insiders.

If one can imagine it, one can prepare for it.

Traficom’s Technology and Strategy unit

ennakointi@traficom.fi

Kirsi Karlamaa, Director of Technology and Strategy
Aleksi Blomqvist, Senior Specialist
Paul Hermansson, Senior Specialist
Henri Jokinen, Senior Specialist
Markus Mettälä, Senior Specialist