Cybersecurity scenarios 2035 – executive summary

Foreword

The cybersecurity scenarios 2035 describe four alternative future worlds in which different outcomes of technological development, interdependencies, the power of large corporations and regulatory success shape the cybersecurity environment in decisive ways in the years to come.

The purpose of this scenario work is to provide a tool for understanding these possible alternative development paths and their consequences for various organisations and actors. This work represents an exceptionally broad perspective of more than 200 experts from the public and private sectors, academia, international partner networks and civil society.

The most critical risks until 2035 may arise when technological dependencies, weak management, the crumbling of identity and the integration of the physical and digital worlds concentrate and accumulate. It is likely that the future of cybersecurity will be decided increasingly in the structures of dependencies, trust and power. In all of the scenarios, AI, supply chains, the reliability of the information environment and the connectivity of critical infrastructures stand out as crucial issues.

The cybersecurity scenarios support preparedness, decision-making and strategic discourse in a situation where the security of the future digital society is based on increasingly complex dependencies.

The cybersecurity scenarios 2035 were produced as part of Finland's cybersecurity strategy. Preparing for the future and strategic foresight associated with this aim are a priority for the Finnish Transport and Communications Agency.

Kirsi Karlamaa
Director of Technology and Strategy

TRAFICOM
Finnish Transport and Communications Agency

Key findings

1. The growing integration of AI into societies may mean that cybersecurity becomes an infrastructure issue. Key elements consist of data, computing, management layers and agent ecosystems as well as their links to critical processes.

2. The reliability of the information environment plays a central role for cybersecurity in all the scenarios.

3. The threat actors of the future may largely be the same as today. Their influence depends on their resources and capabilities for operating in different technological environments.

4. The centralisation or fragmentation of technologies may result in different risk profiles.

5. 6G technologies, space technologies and quantum technologies may change the structure of the cyber environment. They will increase both resilience and the risk of systemic disruptions.

6. The greatest future risks may arise where uncertainties concentrate and accumulate. The most serious situations may result from the intertwining of autonomy, centralised infrastructure, the integration of the physical and digital worlds, the crumbling of identity and a lack of controls.

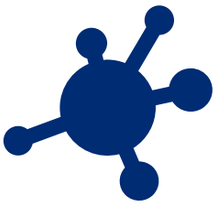
Four future worlds

Torchbearer

In the 'Torchbearer' scenario, geopolitical tensions persist and supply chains have partly become regionalised. The EU is a regulator of technology and cybersecurity and a creator of standards while building a 'third way' between the US and Chinese models that focuses on democracy and the protection of privacy. Strong identification, an EU cloud and data solutions compliant with regulation provide a minimum level of security.

In this scenario, there is a steadfast effort to prevent the fragmentation of the information environment. Transparency and the separation of synthetic and organic content are required of platforms, and environments of verified information that can be accessed by strong identification are built for citizens. The downside of this model is that some actors perceive it as censorship or an 'EU reality' with excessive control.

While technological advancement does not stop, technologies will be introduced at a more moderate rate. The overheated hype associated with large AI language models has died down. The EU manages to improve its self-sufficiency in cloud, AI, quantum, 6G and space technologies. While this does not eliminate the threats, it makes them more manageable.



Fragmentation

In the 'Fragmentation' scenario, the world is split into blocs, supply chains become regionalised and the EU loses its ability to create a common policy on digitalisation and infrastructure. The Member States are divided into different camps, large corporations hamper regulation and technological development advances unevenly. The end result is a patchwork infrastructure that undermines interoperability, management and trust.

The central element of this scenario is a collapse of trust. The public Internet becomes an environment rife with synthetic content, manipulation and scams, which leads people and organisations to turn to more closed solutions. Various platforms create different truths, and the shared foundation of information turns brittle. Citizens also start opposing systems actively through countermeasures such as poisoning sensors and smart features.

In this world, AI has been deployed too fast and without adequate control. Various 'AI disasters' have led to leaks of sensitive data, manipulation and reverse engineering, as a result of which trust in data disclosure erodes and technology deployment is slowed down. Technology is still used, albeit more cautiously, narrowly and suspiciously, while threat actors continue to use AI tools aggressively.

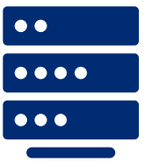
Despite mistrust, dependencies grow stronger rather than decline. Tech giants and major suppliers are the only actors capable of guaranteeing national digital continuity, while their acceptability and trustworthiness is simultaneously crumbling.

Two Realms

The 'Two Realms' scenario describes a world where global digital infrastructure is divided into two blocs led by major powers. The United States is trying to break away from supply chains dependent on China, China is technologically strong, while the EU relies on US technologies and monitoring in its security policy. The EU's technological sovereignty projects remain inadequate, even if more stringent security regulation is brought in.

In this future, security overrides privacy. Control of the digital infrastructure increases, data protection is undermined, and monitoring tasks are also assigned to large service providers. The information environment becomes governed, filtered and ideologically controlled. The space for dissent also shrinks in the name of internal and external security.

In this world, technology follows the logic of an arms race. Autonomous attacks and defence minimise response times, functions that are critical to the security of supply depend on AI control, and 6G, satellite broadband and quantum technology are linked to security architecture. Cybersecurity is part of the power games between major powers, with tech giants providing the tools.



Data Empires

In 'Data empires', global growth is based on mobility, data and business-driven technological integration. Large tech corporations manage to keep value chains stable, mitigate protectionism and also maintain connections with world trade dependent on China. In practice, countries are divided into corporations' spheres of influence, and the EU's role changes from an active regulator to a customer.

At the core of this scenario is a shift of power. Public regulation cannot keep up with the level of abstraction and complexity in technology, which is why data empires start taking over decision-making structures, influencing politics and also offering their AI tools to administrations. While forms of democracy survive, practical administration is increasingly shifted to business-driven black boxes.

In this world, citizens' daily digital lives are built on closed platform environments. Biometric data is a gateway to better services, the ability for critical thinking is stunted, and perceived realities diverge based on income levels and the ecosystem used. Privacy becomes a luxury product: rather than being an automatic right, it belongs to those able to pay.

The logic of cybersecurity measures is selective. Data empires afford the strongest protection to their own data pools and well-off customers, while the basic level offered to the rest may be poor.