# Cyberwatch Finland

## WEEKLY REVIEW

46/2025

**Theme Review** **CYBER SECURITY NORDIC**

Cybersecurity is Built by Small Actions and Management of Large Concepts

# Cyberwatch Finland

## WEEKLY REVIEW

46/2025

- Already traditional Cyber Security Nordic Event was held in Helsinki at the beginning of November.

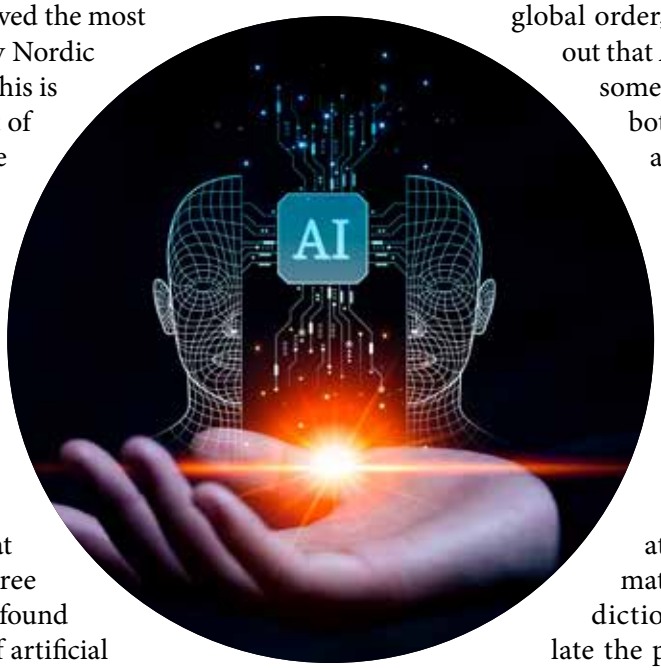
- The event attracted more than 2600 visitors and 75 exhibitors. The event was opened by Finnish Minister of Defence Antti Häkkänen, and in addition to business representatives, there were present e.g. the Minister of Economy and Industry of Estonia.

- The programme dealt with a wide range of different cybersecurity themes, but this year the significance of artificial intelligence and geopolitics was highlighted.

# Introduction

**One of the largest** cyber security events in the Nordic countries, Cyber Security Nordic, was held again at the beginning of November at the Helsinki Exhibition and Convention Centre. This year, the event gathered more than 2600 visitors and 75 exhibitors under the same roof. The program also included dozens of expert speeches, such as opening remarks of Finland's Minister of Defence Antti Häkkänen, Estonia's Minister of Economy and Industry Erkki Keldo and the representative of Taiwan in Finland Freddy Lim. In his opening speech at the event, Minister Häkkänen addressed comprehensive security and tensions in world politics, for example in the context of the war in Ukraine and between China and the United States. Geopolitics and the world situation, together with artificial intelligence, formed two recurring themes in the experts' presentations and programme overall. In addition to the programme solely, the event plays a significant role in bringing together different actors in the cybersecurity field, i.e. companies, authorities and experts. A recurring theme spoken out by experts and heard in the event discussions was the idea that as threats become more diverse, cooperation between different actors in the cyber world plays a significant role in responding to them and gaining an advantage over threat actors.

# Artificial Intelligence as the Top Theme of the Fair




**By far the theme** that received the most attention at Cyber Security Nordic was artificial intelligence. This is not surprising in the midst of the current AI boom, where the threats and opportunities of technology are widely discussed both in Finland and abroad. In the event's programme, artificial intelligence was mentioned in the titles of as many as 16 programme speeches, and only a few presentations did not discuss artificial intelligence at all. Roughly speaking, three clear perspectives could be found for examining the effects of artificial intelligence: the effects of artificial intelligence on societies, its technical operations and its effects on cybersecurity.

One of the best speeches on the societal impact of artificial intelligence was Philip Stupak's speech on national security policy and artificial intelligence. According to his observations, the regulation and risk management of artificial intelligence are still developing, which poses clear challenges together with the different paces of actors. For example, companies would like to make rapid progress in the development and implementation of artificial intelligence, but in the EU, for example, attempts have been made to slow down the development by means of regulation. However, the effects of artificial intelligence are global, and similarly, the most significant artificial intelligence companies operate globally. Stupak threw out the idea of whether even the current political system based on sovereign nation-states is changing with this global phenomena. At the same time, AI will have a significant impact on the labour market, as it will change the work of highly skilled workers, in particular. Some tasks disappear faster than new ones are created. This, of course, creates a challenge that should be addressed. One possible solution proposed by Stupak would be to tax artificial intelligence. This could happen either by taxing the resources used by AI, such as electricity, or by taxing the work it does. The most important thing would be for the relationship between humans and artificial intelligence to be mutually supportive.

**Although Stupak** even saw artificial intelligence as a technology that would revolutionize societies and the global order, several speakers pointed out that AI technology is ultimately somewhat simple. For example, both Geri Revay, a researcher at the information security company Fortinet, and Antti Laatikainen, chief consultant at Reversec, a provider of offensive cybersecurity consulting, stated that the most visible current applications of artificial intelligence, i.e. large language models (LLMs) and generative AI, are ultimately just mathematical models or "prediction machines" that calculate the probabilities of producing the right content. Instead, the concept of agentic AI could be more useful in the future. In this model, artificial intelligence would no longer be a tool, but an independent actor that would be able to operate and make decisions without constant human guidance. This would also have an impact on cybersecurity.

In cyberattacks, the use of artificial intelligence could be described as a race between attackers and defenders. Both Revay and Laatikainen highlighted the threat posed by cyber attacks on artificial intelligence itself, such as promp injections. In them, artificial intelligence is tricked into producing malicious code and thus enables a cyberattack. Revay also highlighted the capabilities of artificial intelligence in social engineering, such as the creation of phishing messages and deepfakes. According to Olli Luotonen from Accenture, who spoke about NATO and attack simulations, generative artificial intelligence is currently involved in about one in six cyber attacks.

**Although AI** was discussed in several speeches through the threats it creates, there are also opportunities for its introduction in cyber defense. According to experts, AI can help cyber defenders find vulnerabilities, and there are examples of zero-day vulnerabilities discovered by AI. At the same time, artificial intelligence could be utilised, for example, in the sharing of threat information, and AI agents could be a significant help in SOC centers. While cybercriminals are quick and unscrupulous to adopt new ways of operating, in the long run, technological advancements could turn in favor for cyber defenders.

# Geopolitics is Also Playing an Increasingly Important Role in the Cyber World

**In addition** to artificial intelligence, another main theme throughout the fair was geopolitics. The topic was discussed or at least touched upon from many different perspectives, but as a whole, it became clear that geopolitics plays an increasingly important role in the cyber world. Katarína Klingová, Research Director at the Slovak think tank GLOBSEC, illustrated the kinds of actors Russia uses in hybrid influencing. As has been said many times, cybercrime against Western countries in Russia is not only accepted, but often state-driven and organised. Often, people who are already in a vulnerable position are lured into the activities either with money or manipulation, and the same applies to hybrid influencing more broadly. Most often, the recruited actors come from the former Soviet territories, but there are also examples of the use of local actors, such as organised crime being involved. It is worth noting that many of those who have committed physical sabotage, in particular, do not know that they are acting for Russia, and only 27% have previously been convicted of crimes.

Another geopolitical state cyber actor that was particularly in the spotlight was China. In a panel on hybrid warfare in the Baltic Sea and Taiwan region, Aapo Cederberg from Cyberwatch Finland, Freddy Lim as the representative of Taiwan in Finland and Jukka Savolainen from Hybrid CoE highlighted that the main goal of China's hybrid operations is to sabotage and impact globally. The idea behind this is that it is easier to control areas that are in disarray. Those familiar with history can see similarities with the Romans' idea of divide et impera, i.e. divide and rule. China's motivation is the competition for world domination, especially with the United States. China's threat should also be taken seriously in Europe, because even though Europe is a much more significant target for Russia, China has the largest economy and the most advanced technology of all threat actors. Although its main focus is on neighbouring areas, it also has the ability to operate in Europe if necessary.

**At the same time,** it is good to remember, as Taiwan's representative in Finland, Freddy Lim said, that in today's world, language and culture no longer offer the same protection to small states as they used to. Ten years ago, Taiwan also calculated that the country would be a much more difficult target for hybrid influencing than average due to these factors, but the situation has changed decisively since then. Finland, as an example, is in exactly the same position, and it should be taken into account more than it is now. The speeches at the event emphasised many times that responding to the wide-ranging influence of a large actor requires, above all, cooperation not only between different countries, but also between the private and public sectors and organisations.

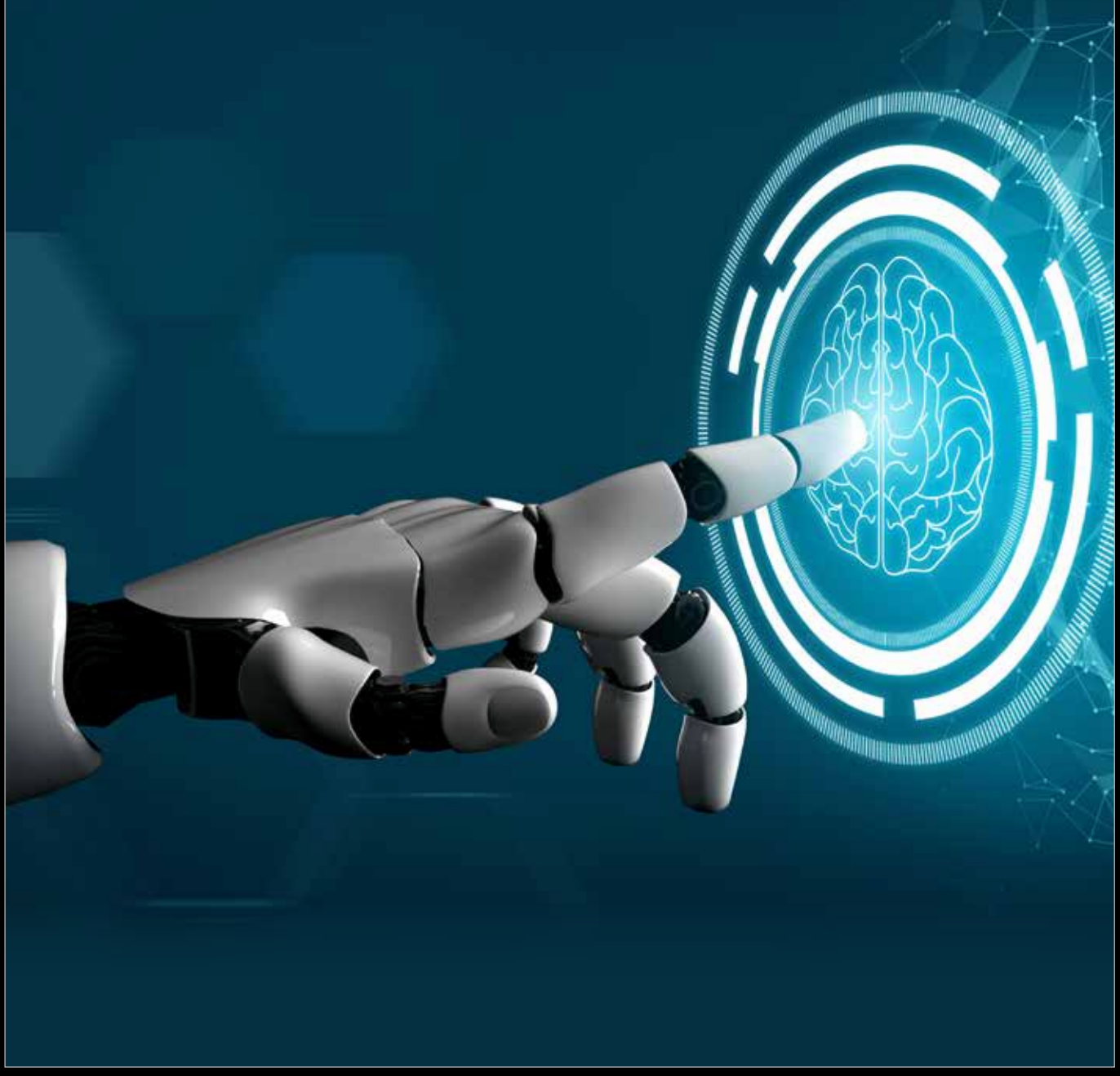
Geopolitics is also linked to the cyber world through technological development. There was concern about the fragmentation of the internet, i.e. that a geographical area would be completely disconnected from the internet. In practice, this would mean that an information network would be introduced in the area in question that is not compatible with the internet that is used worldwide. According to a representative of ICANN (Internet Corporation for Assigned Names and Numbers), there are three factors behind this threat: politicisation, geopolitical instability and new technologies.

**With regard** to politicisation, the prevailing attempt at digital self-determination in many places is particularly worrying. Although the idea itself is to be supported, measures have often been proposed in pursuit that could lead to the fragmentation of the internet. The same applies to legislation and, for example, EU regulation. In particular, ICANN criticizes attempts to address content-level problems by interfering with the internet architecture, which would lead to fragmentation. When talking about geopolitical instability, for example, Ukraine's request to close Russian internet domains, such as sites ending in .ru, was raised in February 2022. The request could not be granted due to the non-political nature of ICANN, but similar cases create a basis for fragmentation. New technologies, such as Huawei's "New IP", can also lead to fragmentation if countries disagree on which technology should be used. Often, there are geopolitical interests behind this, to gain a dominant position for one's own technology.

# Summary

**Every year,** the Cyber Security Nordic Event seems to have a leading theme: in 2023, it was the war in Ukraine, and last year, the NIS2 directive and cyber regulation. This year, artificial intelligence was the clear spearhead. In addition to being present in many presentations, artificial intelligence was also visible at exhibition stands. It seemed that everyone who participated wanted to highlight their own activities specifically through artificial intelligence. Although geopolitics was not quite as prominent, it was present alongside artificial intelligence in the speeches on both days. In addition, the event dealt with cybercrime and how to prepare for and respond to it. Preparedness for and response to cyberattacks were discussed from both a technical and a strategic perspective. It was also interesting to hear the latest figures on citizens' trust and perceptions of digital tools. Roughly speaking, it can be said that many people do think they know how to operate safely in the digital world, even though this is not the case in reality.

In line with the main theme of the event, the rapid development of artificial intelligence is the most worrying digital theme among citizens. The event is perhaps the best place to sense the current atmosphere on digital environment, as the biggest concerns of the participants seem to crystallize time and time again into the theme of the event. It will be interesting to see what will be the most visible theme in next year's Cyber Security Nordic Event.



# Our Aim is to Add Cyber Capabilities in the World


## Contact

Cyberwatch Oy | Nuijamiestentie 5 C | 00400 Helsinki, Finland
aapo@cyberwatchfinland.fi | info@cyberwatchfinland.fi | +358 40 500 8177