

TRAFICOM

Finnish Transport and Communications Agency
National Cyber Security Centre

Information security in 2022



Table of contents

Information exchange, cooperation and preparation	
– Cyber security is created together	3
In 2022, the situational picture, cooperation and information exchange about cyber security were developed and intensified	4
The roles and duties of authorities related to cyber security are clear	5
The development of cyber security is a continuous, strategic activity	5
The National Cyber Security Centre Finland supports the cyber resilience of society as a whole and its different sectors	6
Companies have a major responsibility for maintaining and developing cyber security	6
Cyber security is also a matter of trust	7
Information security in 2022	8
The threat level increased during 2022	9
The number of denial-of-service attacks increased clearly at the end of the year	10
Finnish organisations became victims of ransomware more often	11
Phishing and scams were an everyday occurrence also in 2022	12
With regard to vulnerabilities, 2022 was calmer than the previous years	13
Communications networks were stable in Finland in 2022	14
Cyber espionage attempts continued actively	14
GPS disruptions were reported to Traficom	15
The number of cases of terrestrial radio interference has been decreasing	15

The year 2022 for the National Cyber Security Centre Finland of Traficom	16
Preparedness and cooperation were intensified	17
Network cooperation was developed in 2022	17
International cooperation expanded and continued closely	18
The security of society was promoted with cyber security and digital security development projects	19
The development of exercise activities, situational awareness and forecasting also continued in 2022	20
Attempts were made to increase awareness of cyber threats in many different ways	21
Supporting the development of information security speeds up the improvement of information security in companies critical to the security of supply	22
The Cybersecurity Label was granted to 15 new devices	23
Research and development of cyber security reinforced in Finland and Europe	24
The development of regulation supports cyber security	24
Cyber security trends in 2023	25
How is the rise of the cyber threat level visible in everyday life?	26
The threat of an economic downturn and the lack of cyber talent become a challenge	27
Cyber security procurement expertise must be developed continuously	28
New legislation – it is important to prepare and be proactive	28
How will the information security skills of citizens be supported in the future, too?	29
Our KPIs	30

Information exchange, cooperation and preparation – Cyber security is created together

Now that we are well into 2023, it feels appropriate to sum up the most important cyber incidents of 2022, which was an unusual year in many ways.

Last year, the threat level of cyber security rose higher than it has ever been before. The change has become permanent. The long-term increase in the number of cyber incidents levelled out, but with the war in Ukraine, cyber incidents became more severe and targeted than before. The everyday lives of Finns and the everyday operations of organisations in Finland were impacted by scams, denial-of-service attacks, malware, phishing and ransomware attacks targeting the ICT environments of organisations.

The National Cyber Security Centre Finland (NCSC-FI) of Traficom and other authorities warned about the potential increase of cyber threats over different channels after the extensive attack by Russia against Ukraine in February 2022. The number of serious cyber incidents reported to the NCSC-FI, such as

major ransomware attacks, started to increase significantly in July 2022. The number of such incidents related to functions critical to society in 2021 was low, whereas in 2022 the number of recorded incidents rose to above a dozen. The NCSC-FI supported the affected organisations in their recovery efforts.

In 2023, the cyber security threat level remains high and cyber security is still an important theme in society. Cyber threats spark interest and inspire much public discussion and, understandably, also concern. During this discussion, it is important to talk about the threats and preparing for and responding to them based on accurate and up-to-date information. The authorities have the duty and ability to generate this information.

This review will cover last year's overall cyber security events and phenomena in Finland, the cyber security development measures as well as the activities of the National Cyber Security Centre Finland (NCSC-FI) of Traficom.

” In 2022, cyber security was promoted in many different ways.

In 2022, the situational picture, cooperation and information exchange about cyber security were developed and intensified

Cyber threats do not follow the borders between countries or the different sectors of society. Like other current threats, cyber threats are also wide-ranging in nature and cross-administrative from the perspective of the authorities. Digitalisation has made industries dependent of each other, and few incidents today affect only one single administrative branch or sector of society. Preparing for and responding to modern threats requires that cooperation works well and that the connections between the management, situational picture and communications are in order. Decisions must be made with the right information and based on an accurate situational picture. Cooperation between the different sectors of society related to preparedness and precautions has a long tradition in Finland.

In 2022, the work on developing cyber security was continued by intensifying the cooperation within and between the ministries in charge of security as well as the cyber security authorities. In order to secure the cooperation and information exchange between the authorities and generate a common situational picture, a separate ministry-level group was established in the spring of 2022. The group

is tasked with supporting the decision-making of the state leadership in serious situations involving cyber incidents or cyber influence activities. In addition, duties related to cyber security and the preparedness of public administration were added to the tasks of the Ministerial Working Group on Developing the Digital Transformation, the Data Economy and Public Administration in March 2022.

Traficom, and the NCSC-FI as a part of it, developed the focus areas of their activities to correspond to the increased threat level. New capabilities were developed for technical detection and providing help faster in case of serious cyber incidents. Among other things, the NCSC-FI started to generate a new strategic cyber security situational picture for the needs of the state leadership.

Ensuring the safety and reliability of telecommunications connections and supporting the preparedness of telecommunications operators remained a key objective of the guidance and supervision activities. During the year, several legislative projects were also promoted; their purpose is to develop the information security, risk management and preparedness of companies, support the cyber security co-

operation of authorities and improve the pre-conditions for information exchange.

During 2022, the NCSC-FI intensified its domestic and international cooperation.

We influenced matters in domestic and international networks and participated actively in the preparation and development of legislation. We implemented, coordinated and participated in several cyber security development projects.

The cyber aspect has been closely involved in the extensive attack by Russia against Ukraine in February 2022. The NCSC-FI has monitored and analysed the cyber attacks detected in Ukraine closely and supported the preparedness of the different sectors of Finnish society and their capabilities of responding to different kinds of threats that arise in the cyber environment. One example of this includes the fast reaction cyber preparedness projects, in which rapid first response services were developed along with a new strategic cyber security situational picture analysis, which is shared with the top state leadership, among others. The NCSC-FI has also cooperated closely with Finnish telecommunications operators in order to ensure the functioning of communications networks and services and prepare for different kinds of threats.

The roles and duties of authorities related to cyber security are clear

Work is done to maintain and develop cyber security in Finland every day. The division of labour among the authorities concerning cyber security is clear, and it is based on legislation. Operative cooperation takes place daily, and the authorities have well-organised coordination groups and operating models. In case of a cyber security incident, the National Cyber Security Director together with the ministry-level team generates a situational picture for the state leadership and coordinates the situation. In addition, the Ministry of Transport and Communications coordinates the situation horizontally between the other ministries.

Information and the situational picture concerning cyber security and threats are exchanged constantly with domestic and foreign partners and interest groups. The cooperation between the actors and various sectors of society is close.

The development of cyber security is a continuous, strategic activity

Maintaining and developing cyber security requires investments. It is a long-term, strategic activity, for which up-to-date legislation as well as the cyber security strategy that entered into force in 2019 and the Cyber Security

Development Programme create a good framework and guidelines. The legislation, methods and standards concerning cyber security, preparedness and cooperation between the authorities are developed continuously both in Finland and at the EU level. Education and research on cyber security keep growing stronger in Finland.

Preparedness for and the capability of responding to cyber threats are developed continuously through exercises and by developing regulations. Forecasts of the future are created by analysing technological and social trends when working on scenarios, for example. Without a view to the future, it is difficult to take the right measures proactively and at the right time. The development of cyber security is a strategic activity that is based on an up-to-date situational picture and analysis.

Cyber security is also promoted and supported in many other ways. Examples of these include the so-called information security voucher providing support for the development of information security targeted at companies vital to the functions of society that was decided by the Finnish Government at the end of 2022, the five-year Digital Security 2030 programme of the National Emergency Supply Agency, as well as the development projects funded by the Ministry of Finance from the implementation programme for digital security in public administration 2020–2023 (Haukka).



The National Cyber Security Centre Finland supports the cyber resilience of society as a whole and its different sectors

The National Cyber Security Centre Finland (NCSC-FI) of the Finnish Transport and Communications Agency Traficom guides and monitors the reliability and safety of communications networks and services, the information security of strong electronic identification and trust services as well as the information security and risk management of various digital infrastructure and service providers. We participate closely in the development of both domestic and international regulations and standards on the field.

The NCSC-FI of Traficom is a Finnish authority tasked with generating an extensive information and cyber security situational picture and analysis that cover the different sectors of society and supporting the development of cyber security that crosses the borders of sectors and administrative branches. The strategic situational picture and analysis we generate are utilised widely, such as in the decision-making of the top state leadership and in sectors critical to the security of supply.

The NCSC-FI participates actively in do-

mestic and international cooperation and information exchange on cyber security. In its forecasting and scenario work, the NCSC-FI monitors and analyses extensively the different social and technological development trends that affect cyber security in general, such as the use of artificial intelligence in cyber attacks. The activity supports the preparedness and development of cyber security in the different sectors of society.

The NCSC-FI serves the whole Finland, and its duties include providing general information on cyber threats, such as vulnerabilities in commonly used software. The NCSC-FI produces and continuously updates instructions for both citizens and organisations, which explain how to prevent different kinds of information security incidents, among other things. The NCSC-FI advises companies, corporations and citizens in issues related to information and cyber security and supports pre-trial investigation authorities in investigating cyber crimes. A weekly cyber security review is published on the website of the NCSC-FI every week; it tells about recent observations and factors that affect cyber security. The monthly Cyber Weather report studies long-term cyber security trends. The website of the NCSC-FI also offers instructions for main-

taining and developing everyday cyber security skills for everyone.

The NCSC-FI estimates that its measures on preventing information security breaches and helping citizens generate a significant net benefit for society measured in euros every year.

Companies have a major responsibility for maintaining and developing cyber security

Cyber security and protection as a whole are made up of several different actors. Here, companies play an important role. They are responsible for providing several services that are critical to the functioning of society.

Without service providers in the private sector, electronic communications would not exist in practice – or at least they would not be available to all citizens. For example, telecommunications operators are responsible for the functioning of the mobile connections and offer access to the internet, among other things, via their networks. Without telecommunications operators, terrestrial or cable TV distribution and services would not exist, either. Telecommunications operators and banks offer us mobile certificates and online banking credentials that we can use to log in to e-services and currently also take care of several different matters with the authorities, when necessary.

” The NCSC-FI maintains an extensive situational picture of cyber security.

In Finland, operators are themselves responsible for cyber security in their respective fields of operation together with public authorities. As the operating environment changes, more and more cooperation between the public and the private sector is needed. Such cooperation in cyber security already has a long tradition in Finland both between and within the various sectors of society. This cooperation, which has also sparked interest around the world, has been built and developed systematically in accordance with the principles and concept of comprehensive security. Over the years, the cooperation has been intensified and operating models have been created for it. In addition, the lessons learned from joint exercises are constantly being introduced in practice in the different sectors. Cyber protection as a whole is created by actors who do their tasks well, cooperation and continuous exchange of information.

Cyber security is also a matter of trust

Cyber security also means the trust of people in society, its institutions and services. If people do not trust the services and their information security, they do not want to use them, either. It is important to maintain and strengthen trust. Trust is the glue that holds our society together. This also includes trust in digital

services and cyber security. By doing the right things and communicating openly about them, we can do our part to support keeping the trust. It is also important to talk openly and transparently about problems and errors.

Issues related to cyber security, particularly threats, come up very quickly in public discussion. They both interest and worry people. When talking about cyber security, it is important to discuss it based on accurate and up-to-date information. Such discussion supports and promotes the crisis awareness and resilience of society. Cyber security is being developed every day, and the activities and operating methods are changed according to the changing threat environment. The threats that come up in the cyber environment are constantly analysed and responded to.

2022 was a year with several simultaneous crises. The change in the security environment, the coronavirus pandemic, the energy crisis, the threat of an economic downturn as well as climate change affected every one of us. The financial impact of crises comes up quickly in public discussion, but it is equally important to pay attention to their social and societal effects. These effects may only appear a long time after the fact.

Security is also a feeling. The way people experience and interpret risks and crises may differ greatly from the understanding of the authorities and other actors. The authorities and

other actors in society must meet this need for information by listening and discussing matters as well as with active, open communications at the right time. This also applies to cyber threats.

Cyber threats have a concrete effect on society as a whole, from the level of individuals to the entire society. Disruptions in digital networks or electronic service affect our daily lives. The more friction there is in everyday life and the longer it lasts, the greater the chance it has of affecting the psychological resilience of society. When preparing for cyber threats and talking about them, it is also important to remember psychological resilience.

Finally, it is good to keep in mind that the development of cyber security is like running an ultramarathon. The difference compared to the real-world running event is that in the cyber world, the finish line keeps moving further and further, and new competitors may jump in from the bushes and join the race. To keep up with the pace and succeed, we need endurance, the right equipment suitable for the purpose, a systematic and strategic approach, cooperation between the maintenance crew and other partners, as well as forecasts. We know what the profile of the route is like, and where our fellow competitors are running. We also know how to adjust our pace, maintenance and steps accordingly. We succeeded in this in 2022. Our goal for this and the next year is the same.

Information security in 2022



The threat level increased during 2022

The coronavirus pandemic and the extensive attack by Russia against Ukraine in February 2022 also affected the security situation of Finland. During 2022, our security environment changed significantly. In the spring, the authorities such as the Finnish Security and Intelligence Service issued a warning on the possibility of extensive hybrid influence against Finnish society and its different sectors. The Finnish Security and Intelligence Service also commented on the actors behind certain cyber incidents. Instructions were given to pay special attention to preparing for and responding to cyber attacks and information influence activities in particular. All this was done. On the cyber security side, investments in the development of preparation and readiness were made in the different sectors of society.

The National Cyber Security Centre Finland (NCSC-FI) supported the organisations in this work.

During 2022, ransomware, targeted phishing and malicious traffic increased against both the central government as well as organisations critical to the security of supply. The attack methods also changed. Due to the change, the NCSC-FI highlighted and provided information about the rising threat level in the cyber environment for the first time in September. The action was coordinated together with the Finnish Security and Intelligence Service. In the estimate of the NCSC-FI, Finland has coped well with the rise of the threat level – due to the preparedness culture and an open discussion environment between the authorities, among other things.



Criminal activity is very opportunistic, and criminals keep up with the news. For example, scams were observed during the pandemic in which attempts were made to get people to hand over their information under the pretext of topics and themes related to the coronavirus. The political decisions of states, changes in the security environment and decisions by companies may inspire criminals to target attacks at Finnish organisations.

It is also good to keep in mind that even cyber attacks that are not specifically targeting Finland can still cause spillover effects here due to the global interconnectedness of digital systems.

” Finland has coped well with the rise of the threat level.

The number of denial-of-service attacks increased clearly at the end of the year

During 2022, denial-of-service attacks against Finnish organisations and companies increased in particular. The number of such attacks reported to the NCSC-FI was clearly higher than in 2021. However, a part of this growth was also due to the public discussion that had lowered the reporting threshold.

During 2022, hacktivism and visibly linking the attack to a political ideology were highlighted with regard to denial-of-service attacks. Even though hacktivism as a phenomenon is not new, carrying out a denial-of-service attack as a statement was more visible publicly than in previous years.

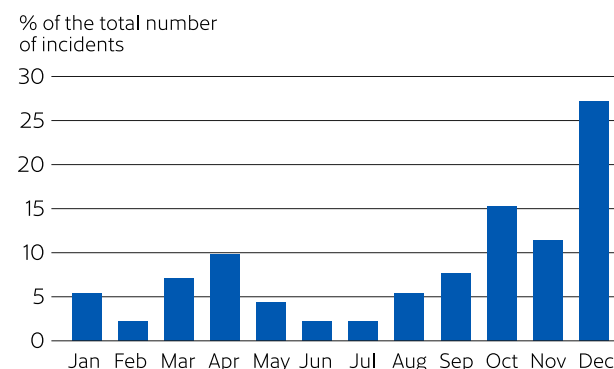
Denial-of-service attacks have been carried out all over the world for a long time, but in 2022, they were harnessed more often as methods of cyber and information influence. Examples of these included attacks targeted at online

services used by citizens; by denying access to them, the attacker could create a public image of a more serious attack than it was in reality.

As a result of the war in Ukraine, denial-of-service attacks carried out as a statement became more common. Many other international political or other significant incidents also inspired hacktivists to carry out denial-of-service attacks. The most visible cases among the attacks in Finland included the attacks by pro-Russia hacktivist groups, such as NoName057(16) and Killnet. The targets included especially actors in the central government as well as the healthcare and social welfare sector, finance sector, transport and logistics as well as media; disruptions in their services were directly visible to citizens, even if they did not affect the internal systems of the organisations and the effect on the external services mostly did not last long, either.

Denial-of-service attacks have already been an everyday occurrence in Finland for years. Every year, more than 10,000 of them are detected. Implementing a denial-of-service attack does not require any special technical expertise; instead, it can be ordered from criminals as a commercial service. As a method, a denial-of-service attack is highly visible and implementing one is an easy way to get publicity. The inconvenience caused by the attack is short-term and they rarely cause any real damage. As an influencing method, a denial-of-service attack is in the grey zone between cyber and information influence.

Reports of denial-of-service attacks processed by the NCSC-FI in 2022



In 2022, denial-of-service attacks were also carried out more persistently than before, and among other things, the attackers started changing their techniques as soon as countermeasures were taken. The NCSC-FI maintained a situational picture of the denial-of-service attacks, assisted organisations in preventing them and provided information publicly of their actual impact. Reports by organisations on denial-of-service attacks to the NCSC-FI increased during the year, and it was possible to carry out protective measures to prevent the impact of the attack against even persistent attacks that used a variety of different methods. One quarter of all of the denial-of-service attacks in Finland during 2022 were reported to the NCSC-FI in December.

Finnish organisations became victims of ransomware more often

In 2022, more cases of becoming a victim of ransomware were reported to the NCSC-FI than the previous year. The cases of the Finnish News Agency STT, Wärtsilä Corporation, Vahanen Group and Uponor Corporation, among others, were highly publicised. Ransomware cases also increased internationally. Trends and phenomena from other countries arrived in Finland, too. Global incidents affected Finland in 2022 more often than before. In fact, some of the attacks were publicly linked to the geopolitical situation.

During the year, the spread of ransomware in Finland was seen as more focused than before, and the malware identified in the cases detected in Finland were also actively used internationally. During 2022, there was an increase in ransomware cases especially during the summer, but during the autumn,

reports of such cases decreased. The number of cases rose again towards the end of the year. During the summer, ransomware attacks clearly targeted against the victim organisation focused on large and important companies, and at the end of the year, actors in the municipal sector also became victims.

Even though the targets of the attacks also included important large companies and organisations critical to the security of supply, the methods used in the attacks were quite ordinary. Most of the attacks leading to ransomware cases were carried out with a phishing message transmitted via email. Advantage of the lack of other common protection methods, such as good password practices or software updates, was also taken in ransomware attacks.

” During the year, the spread of ransomware in Finland was seen as more focused than before.

In 2022, the Finnish News Agency STT received the Information Security Trailblazer award for its open communication and response after becoming a victim of a ransomware attack. Fast and open communication in case of a ransomware attack helps the organisation to resolve the incident and recover from it and also supports other actors in preparing for cyber threats.

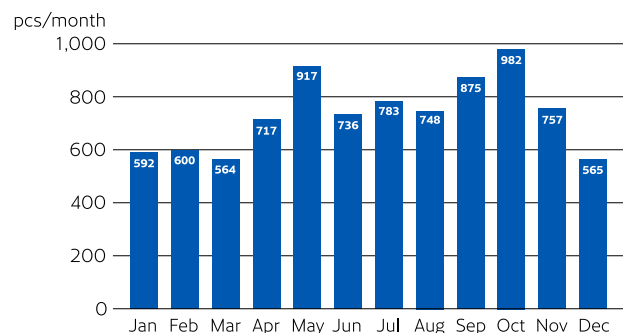
Phishing and scams were an everyday occurrence also in 2022

Attempts at phishing and scams continued actively in 2022, too. During the year, messages were sent in the name of banks and authorities, for instance, attempting to get people to hand over their online banking credentials or credit card or personal data to scammers. The numbers of hijacked social media accounts and hijacking attempts reported to the NCSC-FI continued to increase. The hijacking of social media accounts has been especially harmful to people whose main source of income is linked to a social media channel.

In 2022, new methods were detected in phishing and attempted scams. Certain basic methods were often emphasised in the scams. Referring to urgency, making threats or pretending to be a trusted party are basic methods used in scams in general. Criminals have also used phishing and scams customised to the target; for example, CEO and invoicing fraud has been targeted at companies during the year.

Examples of the new methods observed in 2022 include an extensive scam campaign, in which an attempt was made to replace the account to which the salary was paid with the scammer's bank account. The same scam has been detected before, but now it was attempted systematically. An attempt was made to

Reports of scams and phishing processed by the NCSC-FI in 2022



use a similar scam to transfer rent payments to scammers with a text message campaign in early 2023. In addition, extortion scams using the police as a theme spread to Finland from abroad in 2022. Document attachments decorated with colourful stamps and official titles that had already been found in Europe blatantly threatened people with charges and consequences unless the victim paid a ransom with a virtual currency. Scammers tried to increase the credibility of the scam by using the logo of the Football Association of Finland in a document by a police authority. Another major phenomenon in early 2023 has been phishing for copies of identification documents and thereby also personal data for potential identity theft.

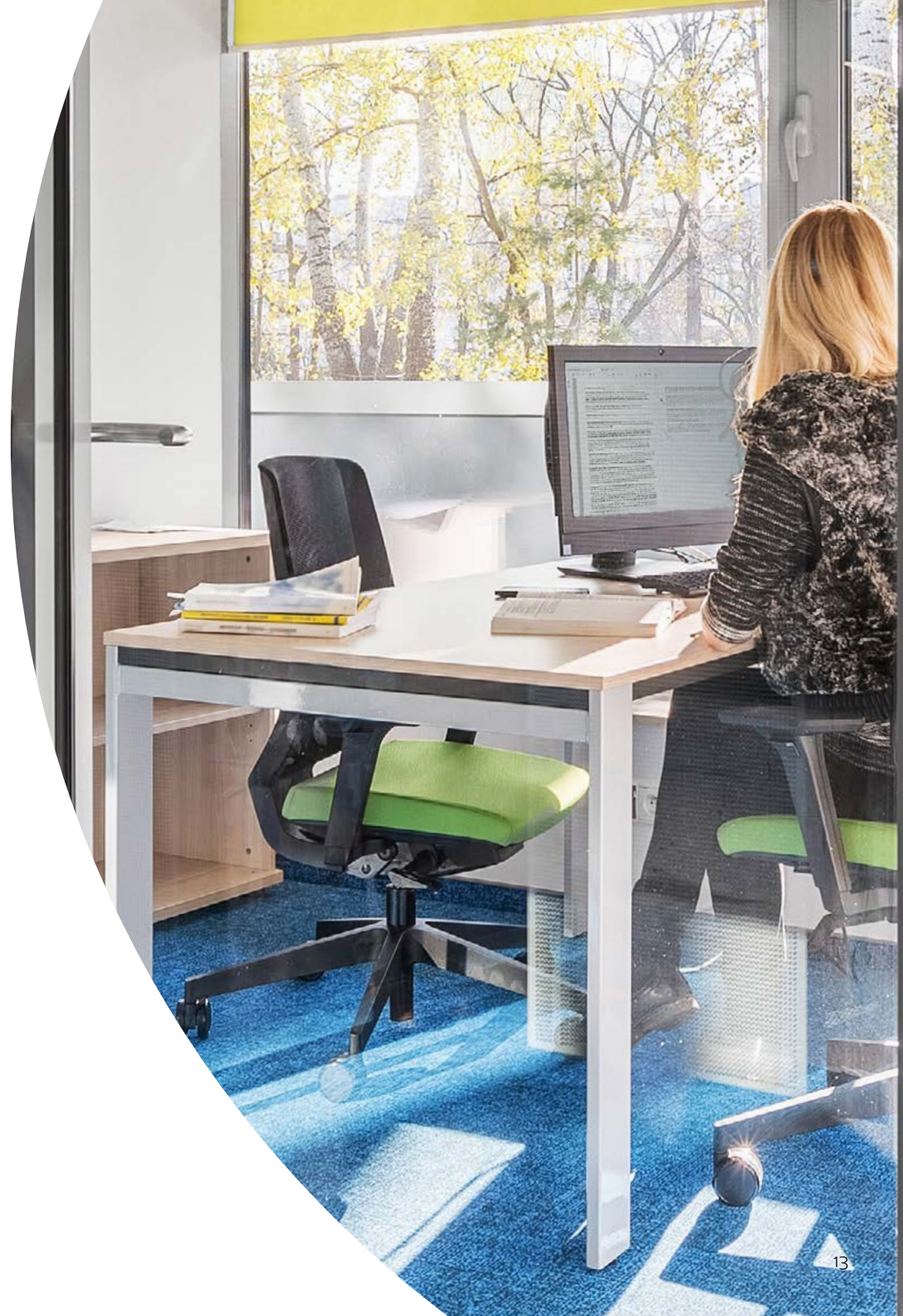


With regard to vulnerabilities, 2022 was calmer than the previous years

The year 2021 is remembered particularly for numerous vulnerabilities that had global impacts, some of which we also published warnings about. In 2022, individual vulnerabilities with a very significant impact on society were avoided. During 2022 we published ten vulnerability notices fewer than during the two previous years.

New vulnerabilities are found constantly. Attempts to exploit vulnerabilities are also carried out with regard to old vulnerabilities. Reports have been made to the NCSC-FI on cases in which vulnerabilities that are several years old have been exploited by criminals. Forgotten updates or incomplete repairs may expose the organisation to many threats. In fact, organisations should identify their own vulnerable systems and keep their software up to date.

On average, we release 1–3 warnings per year, and the only warning in 2022 involved the FluBot malware. In 2021, the number of alerts published was five, which was significantly higher than the average.



Communications networks were stable in Finland in 2022

In 2022, the operation of communications networks in Finland was stable. Clearly fewer service interruptions occurred than during the previous year, and serious interruptions and their consequences were avoided. Individual interruptions caused momentary disruptions of regional services or emergency traffic, but they did not last for long. The number of functionality incidents in public communications services decreased by 38% in total compared to 2021.

The authorities work in close cooperation with Finnish telecommunications operators in building telecommunications connections and securing the functioning of the networks. The regulations that guide construction do their part to ensure the functioning of communications networks in different situations.

The telecommunications connections within Finland and abroad have been secured and protected with several different methods. However, disruptions in the connections are always possible. In case of a possible disruption, telecommunications are directed and managed via other cables or backup systems. The operation is highly automated, meaning that the user may not even notice that there is a disturbance in the communications network.

Cyber espionage attempts continued actively

In 2022, cyber espionage attempts continued actively as in the previous year. Finnish organisations were constantly targeted by activities aiming at identifying the services used and finding different kinds of vulnerabilities or weak passwords. Vulnerable network devices and services have been an object of interest in cyber espionage, because they make it possible to access confidential information and communications or other systems. In addition, targeted malicious email messages are still widely used in cyber espionage. Based on public, commercial, official or other sources, some of the activities indicate actions by state actors.

Russia's attack against Ukraine was visible in cyber espionage and influence in many ways during the year. For instance, several new kinds of malware that encrypt data as well as different kinds of phishing or malware distribution campaigns were detected in Ukraine

Government operators continue to take advantage of vulnerable domestic and small business routers as well as network drive servers as a part of their attack infrastructure. Devices that have not been updated or that are poorly protected and can be accessed via the internet are exposed to malicious actions in general, which is becoming a growing problem. The vulnerable devices are not necessarily exploited against their own users; instead, they can be used to implement more subtle cyber attacks against domestic targets.

during the year. Elsewhere in Europe, cyber espionage has been targeted at actors related to the war and humanitarian assistance, for example. One example of the significant impact of wartime cyber activities outside Ukraine, too, was the disruption in the Viasat satellite service.

” In 2022, cyber espionage attempts continued actively as in the previous year.

GPS disruptions were reported to Traficom

Russia's invasion of Ukraine caused significant changes to flight routes on account of the closure of Russian airspace. Disturbances in aircraft satellite navigation systems were observed in the vicinity of conflict areas in particular. The European Union Aviation Safety Agency EASA published a related [bulletin](#) in March. [A NOTAM message](#) warning all pilots of GPS outages was also published in Finland in early March and cancelled on 15 March 2022.

In 2022, a total of 65 pcs of GPS signal outages or weakening of the signal during the flight of an aircraft in Finland were reported to Traficom. During the previous coronavirus years, 8 pcs of reports were received in 2021 and 27 pcs in 2020. In 2017–2019, a total of nine reports were received. There were 1,327 reports of GPS disruptions received from Finnish aircraft outside Finland. The number of disruptions concerning aviation is monitored and the issue is discussed on an international level as well as by EASA, Eurocontrol and the International Telecommunication Union (ITU). Specific EU-level requirements apply to occurrence reports in aviation with regard to the protection of privacy

of the reporter, among other things. The occurrence reports are also confidential in accordance with the Act on the Openness of Government Activities. No GNSS disturbance notifications related to satellite radio navigation have been received from terrestrial transport sector operators during 2022.

The number of cases of terrestrial radio interference has been decreasing

Overall, the number of cases of terrestrial radio interference has been decreasing. During 2022, a total of 86 cases of radio interference were reported to Traficom, 32 of which needed a field investigation. During 2021, there were 115 cases of interference reported. Of the cases of radio interference reported in 2022, 11 were related to satellite radio navigation (GNSS). Most of these involved reports of GNSS anomalies by private citizens in which a sports watch, car navigator or map plotter, for instance, had shown the wrong location.

In its own monitoring, Traficom detects small jammers regularly all over the country. In 2022, the agency detected 422 jammers.



The year 2022 for the National Cyber Security Centre Finland of Traficom



Preparedness and cooperation were intensified

Due to the change in the security environment and the rise of the threat level in the cyber environment, the authorities intensified their preparedness and cooperation with both domestic and foreign partners. The level of preparedness was raised for Finnish authorities, public administration and critical infrastructure operators. In the spring of 2022, the National Cyber Security Centre Finland provided the management of organisations critical to security of supply with clarifying instructions and support for strengthening their preparedness and continuity management. The Finnish Security and Intelligence Service also told companies to prepare for the threat of cyber and information influence.

During 2022, the cooperation between different information exchange and situational picture information generation and sharing networks was intensified, while investments were made in real-time exchange of information and experiences. The cooperation with telecommunications operators continued in order to secure the functioning of Finnish networks and services. Among other things, the observations made and lessons learned from Ukraine concerning the protection of the communications infrastructure were used in the work.

The cooperation within and between the ministries in charge of cyber protection and the cyber security authorities was intensified further

in 2022. In order to secure the cooperation and information exchange between the authorities and generate a common situational picture, a separate ministry-level group was established in the spring of 2022. The group is tasked with supporting the decision-making of the state leadership in serious situations involving cyber incidents or cyber influence activities.

Network cooperation was developed in 2022

Continuous exchange of information is an essential part of the activities of the NCSC-FI, and it is one of our key service tasks. We participate in several international cooperation groups and facilitate information exchange in Finland in all of the industries critical to the security of supply of society. Information is exchanged on both the most recent cyber threats as well as preparedness in addition to cyber security management.

The most important networks for the NCSC-FI in Finland are the Information Sharing and Analysis Centres (ISAC). They are confidential and independent groups consisting of organisations in a specific industry. There are such groups for the food, energy, financial, ICT, media and water management sectors as well as internet service providers, chemistry and forestry, logistics and transport, and health-care and social welfare in addition to central government. ICT-ISAC was established based

on the wishes of companies in the field in the autumn of 2022. In addition, the users of the monitoring and early warning system HAVARO of the NCSC-FI have their own information exchange groups.

The biggest topics discussed by ISACs during 2022 have included the impact of the war in Ukraine on cyber security, the NIS2 and CER directives of the EU and the DORA regulation, as well as the dependency of society on ICT services produced abroad. The topics were discussed at the meetings of ISACs, and separate surveys on them were also conducted among the members of ISACs. The NCSC-FI used the information obtained in generating the national situational picture of cyber security, and the issues were also reported publicly. By participating actively in the cooperation, the members of the information exchange groups also receive up-to-date information from their peers themselves.

The cooperation between operators and the NCSC-FI that started in 2021 led to issuing a new recommendation early in 2022 concerning different methods for preventing the forging of the caller's number and transmitting scam calls to the recipients of a call in Finland. The goal is to prevent the use of Finnish numbers in international data network crime and reduce the number of scam calls coming from abroad. In fact, according to the National Bureau of Investigation, the number of euros lost due to scam calls has decreased significantly compared to previous years.

International cooperation expanded and continued closely

The aim of international cooperation is to support the generation of the national and international situational picture of cyber security in particular, thereby promoting the achievement of goals for the Finnish cyber security. Reciprocal international information exchange is vital for maintaining and developing cyber security on the national level. Information or warnings of cyber violations or an information system vulnerability, for instance, received from international networks or another country may play a critical role from the perspective of national preparedness.

During 2022, international cooperation was intensified and developed on different levels. As a whole, international cooperation during 2022 was characterised by the war in Ukraine in particular and the highlighted need to share information between the different partner countries. International cyber security cooperation networks also showed their ability to adjust rapidly to changing situations in the security environment in practice.

Finland participates actively in international organisations, institutions and networks. Established trust-based cooperation groups in different geographic areas are em-

phasised in the operative cooperation. The most important cooperation groups include the Nordic Cert Cooperation (NCC) and the European Governmental Certs (EGC) group formed by certain European countries, as well as the global International Watch and Warning Network. In addition, there is extensive international cooperation in different industries in which the NCSC-FI also participates. One example of this is the Nordic Financial Cert cooperation group for Nordic financial institutions.

Cooperation at the EU level is also developing constantly. The NCSC-FI participated actively in the operation of the CSIRT (Computer Security Incident Response Team) network of national cyber security centres between EU Member States that compiles a technical and operative cyber situational picture in the EU. During 2022, cooperation was developed in the EU on a more strategic level especially in the CyCLONE network; its purpose is to generate situational awareness and analyses for the Horizontal Working Party on Cyber Issues of the Council, among other things, especially in extensive cyber crisis situations. In addition to the EU networks,



the cooperation by Finnish authorities with the different cyber security networks of NATO also intensified in 2022.

The NCSC-FI participates in the Executive Board and various expert groups of the European Union Agency for Cybersecurity (ENISA) and it acts as a national ENISA liaison office. The NCSC-FI also has a representative at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) located in Tallinn.

Along with the cooperation networks linked to regulations or operating under established institutions, the NCSC-FI also participated actively in the operation and cooperation of several other international networks, such as the cyber security co-operation between the Nordic countries. The operation of the international networks mentioned is strongly based on trust between the different participating countries. In developing regulations, information and lessons learned are exchanged actively with the Nordic sister agencies and as a part of wider EU cooperation forums.

Along with the development of operative cooperation, the EU has had a record number of cyber security initiatives of projects processed by various working groups during 2022. The most important of these have included promoting sets of regulations on the data protection of electronic communications and identification services, finishing the NIS2 Directive, negotiations on the cyber

resilience regulation and several discussions in working groups for strengthening the protection of critical infrastructure. The experts of the NCSC-FI participated closely in the cyber security development projects, proactive influence and preparation of regulations at the EU level. International exercises were also held actively in 2022. During 2022, the exercises emphasised the strategic level and practicing decision-making processes in crisis situations more strongly than before.

The security of society was promoted with cyber security and digital security development projects

In recent years, the NCSC-FI has implemented several projects for improving the cyber security of actors vital to society and thereby the preparedness as well as the cyber security of society as a whole. In these projects, the National Emergency Supply Agency has played a key role, both in funding the projects as well as supporting their implementation. The development projects funded by the National Emergency Supply Agency are funded through the Digital Security 2030 programme of the National Emergency Supply Agency, and they follow the goals set in the programme. In recent years, it has been possible to expand the cyber security development work when the Ministry of Finance has also participated in the funding and

support of these cyber security development projects. The development projects funded by the Ministry of Finance are funded from the implementation programme for digital security in public administration 2020–2023 (Haukka).

The targets of the development projects funded and supported by the National Emergency Supply Agency include companies vital to society and their cyber security, while the targets of the development projects funded and supported by the Ministry of Finance mainly include operators in public administration vitally important to society and their cyber security. The shared goals of the development projects funded by the National Emergency Supply Agency and the Ministry of Finance include the offering of new information, tools and services that help critically important actors in both the public and the private sector to prepare, maintain, develop and improve their own cyber security and thereby the cyber security and safety of society as a whole. The inclusion of the Ministry of Finance in cyber security development projects and the intensification of cooperation have resulted in significant synergies and savings, when the information, tools and services created in the development projects have been cross-utilised in developing and improving cyber security both in the private and the public sector, and there has been no need to implement the same development projects separately for the private and the public sector.

The development of exercise activities, situational awareness and forecasting also continued in 2022

When preparing for and responding to different kinds of disruptions, it is important that the connections between management, communications and the situational picture work well and the roles and responsibilities are clear and have been trained. In 2022, the development of situational awareness continued by means such as developing the forecasting of the operating environment and the Cyber Climate. The aim of the Cyber Climate is to develop the ability of the NCSC-FI to use data and information to create a national situational picture of cyber security, new services and operating models, and respond to cybersecurity threats and security incidents.

The forecasting work focused on taking advantage of artificial intelligence in cyber attacks and crime and estimated when and in what form the effects of the technology would start to become visible. As another special theme, the cyber security and risk management of implementing local mobile networks was discussed in the forecasting work. It is likely that in the future, many actors critical to the

functions of society will take advantage of local mobile networks tailored to their own needs in order to digitalise their operations and make them more efficient. New kinds of risks and competence requirements are linked to these network implementations, and it is important to take them into account in implementing the networks. Publications on the themes mentioned above were also produced for the² website of the NCSC-FI.

With regard to forecasting, the building of cooperation with various actors also continued. As the operating environment changes and becomes more complex, the role of cooperation in identifying future phenomena and their different effects is emphasised further. Cooperation supports the sharing and use of information in all activities.

During 2022, the development of the HAVARO and Kybermittari services continued. HAVARO observes serious information security threats targeted at Finnish companies and issues warnings about them. Kybermittari (Cybermeter) is a national cyber security

assessment model that enables continuous assessment and development of the cyber security of organisations and comparing it between the actors in a reference group.

Several cyber exercises were held in 2022. Even good operating models and instructions may not be enough, if people do not know how to use them in a real situation. With practice, good and accurate process models can be implemented easily in the operation of the organisation in practice, which has clearly increased interest in cyber exercises. In fact, several industry-specific joint cyber security exercises were held in 2022. Organisations see themselves more clearly as a part of a larger network of organisations or a supply chain, which is why practicing joint processes together with partners has recently been considered more important than before. The NCSC-FI supports cyber exercises by offering advisory services, instructions and ideas for scenarios as content for the exercises and supporting the planning and implementation of nationally significant joint exercises.

¹ Artificial intelligence will shape future cyberattacks | Traficom (kyberturvallisuuskeskus.fi)

² New instructions shed light on cyber threats concerning local mobile networks and the management of risks | National Cyber Security Centre Finland

Attempts were made to increase awareness of cyber threats in many different ways

During 2022, attempts were made to increase awareness of cyber threats in Finland actively. For example, various authorities, companies and organisations communicated regularly about cyber threats and provided and published instructions and warnings on the current cyber security situation, such as scam messages detected.

Issues related to the activities of the NCSC-FI, cyber threats and the current security situation were communicated actively via the different communication channels of the NCSC-FI, such as its website and social media. During 2022, several events were held, such as the Cybersecurity Label and Information Security Seminars, whose aim was to increase the knowledge of the Finnish information security community and management on the future regulations in the field of cyber security and information security, changes in the security environment and their effects on cyber security. The Information Security Seminar held together with the National Emergency Supply Agency in October attracted more than 1,000 participants. The main speaker of the event was George Dubynskyi, Deputy Minister of Digital Transformation of Ukraine.

In 2022, a new weekly review of cyber security was launched, in which information

about current cyber phenomena is shared.

The Cyber Weather report published monthly discussed the important information security incidents and phenomena of the past month. The product is primarily targeted at persons responsible for information security, but the everyday cyber security section includes good advice for everyone. The review offers a quick overview of what has occurred in the field of cyber security. The Cyber Weather report was revamped at the end of the year. In the future, the product will be targeted at organisations, and it creates a comprehensive whole together with the weekly review so that topical themes are highlighted in the weekly review to share the information quickly. As for the Cyber Weather, it gives a brief summary of the events of the month while focusing on short- and long-term trends as well as the threats against which the organisations should prepare.

Cyber threats are constantly taking on new forms. The awareness of organisations, information security professionals and the general public to identify and respond to cyber threats and improve their own information security was supported by publishing several guides and instructions on the website of the NCSC-FI. The guides and instructions published in 2022 included e.g. instructions for the management in case of a ransomware situation, a review of the denial-of-service attack situation, instructions related to leaked IDs, an overview of securing the power supply of communica-

tions networks and a description of the international telecommunications connections in Finland and preparing for threats against their functionality. Tips on how to identify information influence were also published in addition to instructions on using multi-factor authentication to protect user accounts.

During 2022, the NCSC-FI implemented or participated in several communications campaigns. They included e.g. the 'Älyä ostoksiin' (smart consumer) campaign implemented at the end of the year, aimed at increasing the knowledge of consumers on information security issues related to smart devices, and the European Cybersecurity Month implemented in October. In addition, the Finnish Broadcasting Company YLE sent an info video on identifying cyber and information influence as a non-profit advertisement on its TV channels in the autumn.

The experts and management of the NCSC-FI gave lectures regularly in national and regional national defence courses on topics related to cyber threats and preparing for them. Experts also gave interviews regularly to domestic and foreign media and appeared in seminars and events both in Finland and abroad. We cooperated closely with universities and other educational institutions in the field. With active and open sharing of information, we did our part to support the dissemination of information and expertise on cyber security in society.

Supporting the development of information security speeds up the improvement of information security in companies critical to the security of supply

In October 2022, the Finnish Government issued a decision on fixed-term support for the development of information security intended for companies critical to the security of supply, i.e. the information security voucher. The purpose of the support is to raise the level of information security of companies rapidly and thus improve Finland's overall resilience against cyber security threats. The National Cyber Security Centre Finland (NCSC-FI) of the Finnish Transport and Communications Agency is responsible for granting the support. Systems and processes that enable applying for, processing and paying the support electronically were developed in the Agency with a fast schedule for applying for and granting the support. This makes it possible to grant the support as quickly as possible for the companies that apply for it.

” The purpose of the support is to raise the level of information security of companies rapidly and thus improve Finland's overall resilience against cyber security threats.

The applications for the information security voucher started in December, and already during the first few weeks the total number of euros in the support applications exceeded the appropriation of six million euros allocated by the Finnish Government for the purpose. The actual processing of support applications started in 2023, and the first positive support decisions were made in January 2023. After the support applications have been processed, the NCSC-FI is responsible for processing the reports on the use of the support by the companies to which it was granted. At the same time, the measures implemented and benefits gained with the support will be assessed.



The Cybersecurity Label was granted to 15 new devices

The Cybersecurity Label published by the National Cyber Security Centre Finland (NCSC-FI) of the Finnish Transport and Communications Agency Traficom in 2019 indicates that the product or service with the label meets Traficom's requirements for a good basic level of information security. The requirements of the label are based on a European standard. The label can be granted to a consumer device that can be connected to the internet, i.e. an Internet of Things (IoT) device. These include smart TVs, smart bracelets and household routers, for example. In 2022, the Cybersecurity Label was granted to 15 new devices. Currently, a total of 25 devices have the label. For its part, the cooperation with the cyber security authority of Singapore that started in 2021 increased the number of labels. The importance of the role of the Cybersecurity Label in indicating the information security of devices will be reduced with the changes in EU regulations that will enter into force in the coming years. The NCSC-FI of Traficom will prepare to change its operations to meet the duties in accordance with the regulations mentioned above.



Cybersecurity



Research and development of cyber security reinforced in Finland and Europe

The European Cybersecurity Industrial, Technology and Research Competence Centre's National Coordination Centre officially commenced operation at the start of 2023 under the National Cyber Security Centre Finland (NCSC-FI) of the Finnish Transport and Communications Agency. The preparations for the Finnish National Coordination Centre started in the autumn of 2022. The Coordination Centre helps Finnish operators participate in cross-border EU projects and obtain EU funding according to national priorities. In addition, the Coordination Centre grants Finnish operators funding for activities aiming to improve cyber security.

The National Coordination Centre is a member of the EU-wide Network of Coordination Centres led by the European Cybersecurity Competence Centre. The purpose of the Network is to improve national cyber security capacities, support cyber security research and accelerate technological development in the EU. The Network of National Coordination Centres increases cooperation between the Member States. This cooperation reinforces the EU's cyber security capacities and the competitiveness of the cyber security sector. The National Coordination Centre is financed by the EU and the State of Finland.

The development of regulation supports cyber security

Taking care of the preparedness and information security of public communications networks and services (i.e. telecommunications operations) has been a part of the legislation as well as guidance and supervision of the operators by the authorities already since the 1990s. The NCSC-FI of Traficom guides and monitors the electronic identification and trust services and providers of digital infrastructure and service providers referred to the EU Network and Information Security Directive (the NIS Directive). The NCSC-FI also monitors the realisation of the protection of confidential electronic communications.

The NCSC-FI issues regulations that specify legislation for the operators it supervises. The regulations are reformed regularly to correspond to the changes in the cyber security environment and technological development. An example of this is the reformed regulation on electronic identification and trust services

issued in 2022. In addition, the NCSC-FI guides the operators it monitors by issuing recommendations and instructions and supporting them in interpreting the legislation.

The NCSC-FI monitors its field often in different ways, such as collecting disturbance notifications, issuing decisions on supervision and conducting inspections. You can read more about the guidance and supervision activities of the NCSC-FI on our website: <https://www.kyberturvallisuuskeskus.fi/en/our-activities/regulation-and-supervision>

In 2022, the NCSC-FI processed hundreds of disturbance notifications and dozens of complaints concerning the use of cookies on websites. The NCSC-FI gave daily advice on compliance with the legislation and issued statements on dozens of requests on the development of legislation, among other things. The centre carried out well-working cooperation continuously with the companies it supervises.

” The National Coordination Centre is a member of the EU-wide Network of National Coordination Centres maintained by the European Cybersecurity Competence Centre.

Cyber security trends in 2023

In 2023, it is very likely that the threat level of the cyber security environment will remain elevated and the technological development will continue rapidly. The regulations will become stricter, and companies will have to comply with the increasingly strict regulations in the field of cyber security. This requires time and resources. At the same time, the threat of an economic downturn is looming, and there is a lack of cyber talent. Companies must protect their information and systems from the growing cyber threats, and they must also make significant investments in cyber security. In addition, companies and organisations must solve new kinds of cyber security challenges, such as scam attempts with deepfake videos and combating bot attacks.



In 2023, criminals will try to use and introduce new technology in order to achieve their goals more efficiently than before. At the same time as artificial intelligence becoming more common and mundane creates new kinds of attack opportunities and methods, it also offers new tools for combating them. For instance, AI-based chatbots offer an effective tool for combating scams and frauds. These bots can identify suspicious messages and warn users from potential scams. This is important, because scammers are becoming increasingly more creative and invent new ways to access information and money.

The cyber defence systems developed, such as machine learning and data analytics, will become increasingly important for cyber security in the next few years. These systems offer real-time, proactive protection against information security attacks. This is necessary, because scammers also use more and more advanced methods and bot systems to attack information systems. The cyber defence systems that have been developed offer significant protection against such attacks.

How is the rise of the cyber threat level visible in everyday life?

The rise of the cyber threat level is visible in the everyday activities of different parties in several different ways. The most important ones include:

-  **Increased information security risk:** Companies and other organisations must protect their information and systems from growing cyber threats.
-  **Stricter regulations:** In the coming years, more regulations in the field of cyber security will be targeted at companies and organisations, which requires resources and expertise.
-  **Investments in cyber security:** Companies and organisations must prepare to make new investments in cyber security so that they can protect their information and systems.
-  **Challenges brought by new technology:** Companies and organisations must solve new kinds of cyber security challenges, such as combating deep-fake videos and bot attacks.

In order for the companies and organisations to be able to meet these challenges, they must make the following changes:

-  **An up-to-date information security strategy** that meets the latest cyber threats is needed.
-  **Investing in training and personnel:** More and more must be invested in the training and cyber security expertise of the personnel.
-  **Ensuring regular cyber risk assessments and development:** Companies and other organisations must ensure that their cyber risks are assessed regularly and develop their systems and processes as needed.
-  **Cooperation with partners:** The effectiveness of cyber security can be increased in cooperation with partners and by taking advantage of the solutions they offer.

The threat of an economic downturn and the lack of cyber talent become a challenge

Due to the potential economic challenges in the near future, the ability of companies and other organisations to acquire and maintain the necessary cyber security resources becomes a challenge. As a result, actors may prioritise savings in the field of cyber security and not carry out some measures. It is likely that this will lead to issues such as an increasing use of outsourcing and supply chains in companies, and along with the need for savings, their further pruning and prioritisation.

The lack of cyber talent will hinder the ability of companies and other organisations to react to and resolve cyber threats and makes them even more vulnerable to attacks than before. Therefore, it is important for companies and organisations to prepare for and adapt to these challenges by developing effective and flexible solutions as well as acquiring and training enough competent human resources.



Cyber security procurement expertise must be developed continuously

Companies and other organisations must develop their cyber security procurement expertise continuously. For instance, this requires that companies have the ability and competence to coordinate the cyber security needs together with the business needs.

Purchased services and supply chains may play an important role in solving the cyber security issues of companies. They offer a chance to outsource a part of the cyber security responsibilities and take advantage of expertise and technology that the organisation itself may not have.

When buying cyber security products and services, organisations must ensure that they meet the functional and quality requirements set for them. This requires an understanding of the different aspects of cyber security and the related standards, technologies and operating methods. In addition, the party acquiring the product or service needs knowledge about the available services and products, the price level and offers on the market as well as an understanding of information security and data protection issues. The party acquiring the product or service must also have the expertise to assess the reliability of the service provider and its ability to offer continuous support and updates.






Are there easily adoptable best practices for the information security and data protection requirements used in procurement? Yes. They include e.g. information security directives and regulations of the EU, the NIST Cybersecurity Framework and the ISO/IEC 27001 and 27002 information security standards.

New legislation – it is important to prepare and be proactive

Companies and other organisations should prepare for regulations changing and becoming stricter. This is necessary, because cyber attacks are becoming increasingly common and more complex. Legislation helps with protecting private and business information and improving overall information security and functionality. Good information security can be turned into a competitive advantage.

EU regulation in the field of cyber security will increase. In February 2022, the Radio Equipment Directive (RED) was supplemented with local information security requirements. It includes a transition period for manufacturers, after which wireless devices placed on the market must meet the requirements starting from 1 August 2024. The NIS2 cyber security regulations on critical infrastructure will enter into force on 18 October 2024.

Companies should do the following to prepare for the EU cyber security regulations in 2023:

-  **Learn about the regulations and prepare for their national implementation:** Companies should find out about the future regulations, such as the RED Directive and the NIS2 cyber security regulations, and determine what requirements they set on the companies themselves.
-  **Assessment and risk management:** Companies should evaluate their current cyber security levels and identify potential deficiencies in following the regulatory requirements.
-  **Planning and implementation of measures:** Companies should plan and implement the measures necessary to comply with the regulation requirements, such as updating the information security software and processes.
-  **Training and communications of the personnel:** The personnel of companies should be aware of legislation and its requirements. Sufficient training and information should be offered to the personnel to comply with the regulations.
-  **Cooperation:** Companies should, in cooperation with the actors in the field and potential support services, prepare for upcoming regulations and comply with them effectively.

How will the information security skills of citizens be supported in the future, too?

As society is quickly becoming increasingly digitalised, information security skill management and their continuous development are important civic skills. More and more often, private individuals are targeted by cyber attacks such as phishing, data breaches, attempts to hijack social media accounts, ransomware and scam messages. This also includes the various forms of information influence, such as spreading disinformation. For this reason, it is important to invest in maintaining and developing the information security skills of citizens as well as maintaining and developing their media and technological literacy.

The cyber security skills of citizens vary significantly. Some need help with basic issues, such as password and software updates as well as identifying scams. Others have excellent information security skills. The National

Cyber Security Centre Finland (NCSC-FI) supports the cyber skills of all of the information security levels.

Cyber security also involves trust. If people do not trust services and their information security provided by a company or organisation, they do not want to use them, either. The more digitalised society and the services it offers become, the more important it is to pay attention to good information security and maintaining trust.

Active, open and regular communications will help with maintaining trust. Both good things and problems must be communicated openly and transparently.

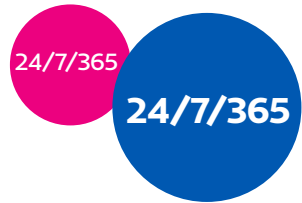
In a digitalised society, attention must also be paid to the realisation of inclusion. How can we ensure that everyone is a part of the digital society? How can we secure the participation and inclusion of different population groups?

” Active, open and regular communications will help with maintaining trust.

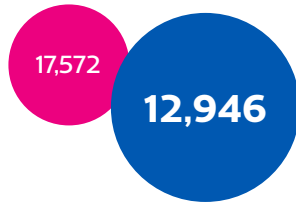


Our KPIs

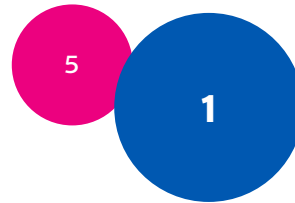
● 2021 ● 2022



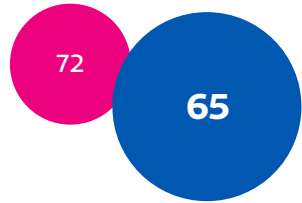
Uninterrupted on-call duty



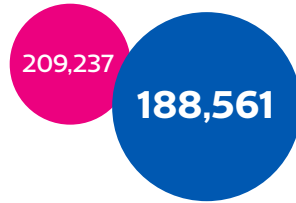
Cases processed



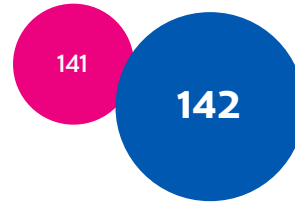
Alerts



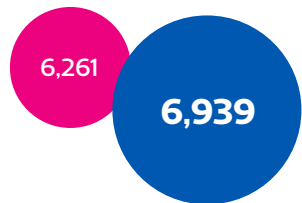
Cases processed by vulnerability coordination



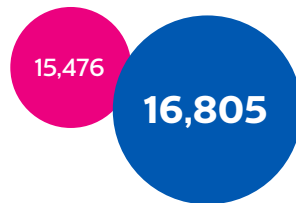
Autoreporter



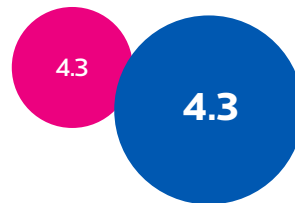
Media contacts



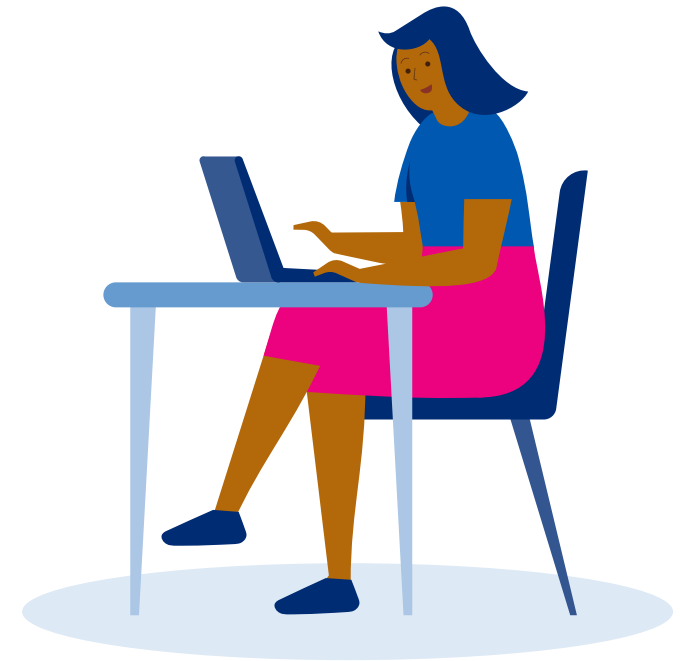
Facebook followers



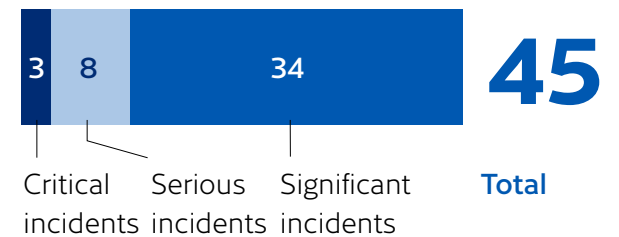
Twitter (now X) followers



Customer satisfaction with our situational picture products



Number of incidents



**Finnish Transport and Communications Agency Traficom
National Cyber Security Centre Finland**

PO Box 320, FI-00059 TRAFICOM
Tel. +358 29 534 5000

[Kyberturvallisuuskeskus.fi/en](https://www.kyberturvallisuuskeskus.fi/en)

Traficom publications 16en/2023
ISSN 2669-8757 (online publication)
ISBN 978-952-311-893-5

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre