



# DIGITAL SECURITY 2030



# **DIGITAL SECURITY 2030**



## [www.huoltivarmuus.fi](http://www.huoltivarmuus.fi)

Security of supply refers to society's ability to maintain the basic economic functions required for ensuring people's livelihood, the overall functioning and safety of society, and the material preconditions for military defence in serious disruptions and emergencies.

The National Emergency Supply Agency (NESA) is an organisation operating under the Ministry of Economic Affairs and Employment. It is tasked with planning and measures related to developing and maintaining security of supply.

The National Emergency Supply Agency operates in conjunction with the National Emergency Supply Council as well as individual sectors and pools that operate as permanent cooperation bodies. Together they form the National Emergency Supply Organisation.

Publisher: Huoltivarmuuskeskus  
Images: Shutterstock  
Layout: Up-to-Point Oy  
Year of publication: 2021

## Table of contents

<b>Part 1:</b>	Foreword/Introduction.....	<b>4</b>
<b>Part 2:</b>	Programme Vision .....	<b>5</b>
<b>Part 3:</b>	Changes In The Operating Environment .....	<b>6</b>
<b>Part 4:</b>	Strategic Priorities And Goals Of The Programme.....	<b>7</b>
<b>Part 5:</b>	Programme Impact.....	<b>10</b>
<b>Appendix 1:</b>	Framework And Priority Of The Programme's Projects.....	<b>11</b>

# PART 1: FOREWORD/INTRODUCTION

**The purpose of the National Emergency Supply Agency's Digital Security 2030 programme is to develop society's tolerance for cyber disruptions. The programme provides projects that develop digital security with funds of about EUR 130 million until the end of 2025. The programme is part of the accomplishment of the strategic goals of the National Emergency Supply Agency and the implementation of Finland's Cyber Security Strategy.**

Cyber security has a key role in the crisis tolerance of the entire society as digitalisation permeates all aspects of society and all sectors of the economy. Consequently, it makes us more dependent on global digital ecosystems and international system suppliers.

Risk identification and foresight is increasingly more difficult and disruptions spread fast, affecting other areas in addition to the target of the attack. Cyber-attacks and influencing are also part of global politics, and the methods of misusing digitalisation are changing rapidly. Furthermore, ensuring the reliability and integrity of information becomes increasingly important as cyber-based influencing increases. A shift from individual systems to securing entire function chains and processes must be made in preparedness and continuity management efforts, which requires cooperation.

The priorities of the programme are preparedness for cyber disruptions, functionality in the event of a disruption, cooperation between different parties in society and business and foresight for future phenomena. The priorities are presented in more detail later on in this document.

The priorities, goals and first projects of the programme have been defined in close cooperation between representatives of and experts from different sectors. The programme is based on the KYBER2020 programme carried out in 2017–2020 and the lessons learned from it as well as the National Emergency

Supply Agency's scenarios of the future that emphasise the impact of changes in the digital operating environment on society. The scenarios represent well the needs of companies and other stakeholders to secure digital security of supply in the midst of changes. The cyber security of critical functions and solutions for foresight related to everyday cyber security is vital. The programme plan has been prepared in cooperation between the National Emergency Supply Agency and the National Cyber Security Centre.

The purpose of the programme is to find solutions and encourage putting these into practice. Through the projects to be carried out, companies are supported in establishing sustainable cooperation structures and operating methods as well as nationally viable business and networks where companies and authorities can work together. The purpose of the projects included in the programme is to generate long-term benefits related to security of supply by supporting the initiation of activities on market terms that support security of supply.

The goal is to use the funding granted through the programme to encourage other parties to invest in cyber security as well, which will amplify the societal impacts of the investment. In order for the programme to succeed, companies and other partners must commit to the accomplishment and implementation of the programme's goals. Together, we can build a society that withstands cyber attacks.



## PART 2: PROGRAMME VISION

The vision of the programme is “Critical functions of our society withstand cyber disruptions”. The vision is a summary of the desired long-term effects of the projects included in the Digital Security 2030 programme. The cornerstones of the vision define the basic preconditions that must be met in order for the vision to be accomplished successfully.



5

### Functions critical to our society withstand cyber disruptions



### Cornerstones of the vision

*There are three key cornerstones related to the successful accomplishment of the vision*

- 1) companies that have the ability to withstand cyber attacks*
- 2) national cooperation networks that support the tolerance to disruptions of companies and society*
- 3) international cooperation networks that support national capacity*



## PART 3: CHANGES IN THE OPERATING ENVIRONMENT

**The programme addresses the constant changes in the operating environment, which are apparent in the scenarios of the future up to 2030 made by the National Emergency Supply Agency. Digital networking of society, strong global system ecosystems, cyber attacks and developments in technology all have an effect on the critical functions of society, the preparedness of companies and protection.**

In a digitally networked society, critical functions are based on automation, machine learning and evolving artificial intelligence. The focus of the development of systems that support the functions and the preparedness and continuity management of the production phase is often on technical safeguards, which may result in shortcomings in planning the protection of the entire function. A shift from the narrow system orientation of preparedness practices and continuity management to the protection of entire function chains and processes is required.

We are increasingly dependent on global digital ecosystems and international system suppliers. Geopolitical technology blocks and disruptions in trade policies mean that national parties must develop international partner networks actively.

Cyber attacks and influencing are part of global politics, and the methods of misusing digitalisation are changing rapidly. In a complex infrastructure, the identification of risks and foresight suffer, and disruptions spread faster, affecting other areas in addition to the target of the attack. Cyber attacks weaken society's trust in digital services. Ensuring the reliability and integrity of information becomes increasingly important as cyber-based influencing increases.

Developing technology requires an agile and flexible mindset from companies, authorities and legislators. The private sector reacts to the development opportunities presented by technology in a business-oriented manner. Legislation is used to secure functions on which society has built dependencies.



# PART 4: STRATEGIC PRIORITIES AND GOALS OF THE PROGRAMME

## Changes in the operating environment

- Management of digital ecosystems is global
- Dependence on automation, machine learning and artificial intelligence
- Risk management in a complex infrastructure is becoming more complicated
- Disruptions spread in an uncontrolled manner
- Critical functions are based on a partner network
- Trust in digital services is jeopardised



### PREPAREDNESS

The dependencies of critical digital infrastructure and services are understood to ensure their functionality



### FUNCTIONALITY

The exchange of information is supported by comprehensive observation and analysis skills and the tools required for this



### COOPERATION NETWORKS

Information exchange networks are active and comply with the defined information sharing models and responsibilities



### THE FUTURE

New phenomena affecting security of supply are studied in cooperation with companies and research and educational institutions

## VISION

Functions critical to our society withstand cyber disruptions

Changes in the operating environment, the programme's vision and the needs of companies form the basis for the programme's strategic priorities. The priorities help define the key objects that are to be accomplished through the projects of the programme.

The Digital Security 2030 programme is built on four key priorities:

1) preparedness, 2) functionality, 3) cooperation networks and 4) the future. Each priority has specific themes, goals and mind-set until 2026. Preliminary plans for projects have been made for 2021 and 2022. The projects of the programme will be specified according to the plan on an annual basis. Some of the projects described in this document are in a planning phase and are subject to significant changes in their implementation. Project themes are updated whenever necessary to advance the goals of the programme according to the results already gained.

The protection of functions and tolerance to disruptions are emphasised in setting the goals. These goals are gained e.g. by anticipating threats, forming an overall situational picture and understanding dependency chains and through international cooperation.

## Preparedness


*Key goals regarding preparedness include comprehension and protection of digital infrastructure and service dependencies and practising the implementation of shared operating models. The preparedness of companies and the need to increase their cyber and digital expertise are also included in this priority.*

As the infrastructure, technical environment and different parties become networked, the National Emergency Supply Organisation has to gain a wider understanding of the dependency relationships of digital infrastructure and services and any possible risk clusters. Critical digital services, such as cloud and authentication services, must be secured, i.e. kept available or restored or replaced with similar services quickly.

In order to accomplish the goals specified above, an analysis of the security of new technologies and technologies with national or international dependency relationships (including telecommunications connections and cloud services) must be made. The operating reliability and replaceability of digital services and communication networks must also be developed.


A key part of preparedness is active cooperation between authorities and companies. Operating models developed together form the basis of national exercises. Exercise activities will be developed and increased regionally, nationally and internationally according to the dependencies of sectors.

Security expertise must be an integral and cross-cutting part of the expertise of the management, expert groups and other staff of companies. In order to develop the required expertise, companies can be offered e.g. sector-specific benchmark data of data security or tools for evaluating the data security of




## PREPAREDNESS

- The dependencies of critical digital infrastructure and services are understood and secured
- Cyber risks in networks are managed throughout lifecycles
- Expertise and understanding of cyber environments is advanced in society
- Regular exercises are part of the planned preparedness development




## COOPERATION NETWORKS

- Active information exchange networks use common information sharing operating models
- Parties know their responsibilities and roles within the network
- International cooperation supports national security of supply
- International data resources are used actively



## FUNCTIONALITY

- Observation and analysis skills are improved
- Sectors react to observations appropriately
- Tools make the exchange of information and shared situational picture more efficient
- An operating model in the event of an extensive cyber disruption is taken into use



## THE FUTURE

- The effect of new phenomena on security of supply is identified
- Research and educational cooperation between companies and research and educational institutions generates data and experts that address the needs of critical infrastructure
- Areas of development in securing digital safety are identified on the basis of the results of research

goods and services. The level of companies' preparedness is also improved by defining sector-specific recommendations for the baseline level of cyber security.

The programme increases the understanding of parties critical to security of supply about the best international practices of selecting technologies and the recommended standards. In addition, the suitability of the practices and standards for sector-specific baseline levels is analysed.

## Functionality

*The key goals of functionality include improving the capabilities of observation and analysis, information exchange and management of the shared situational picture. The management of disruptions and identification of information-based influencing by technical means were also highlighted.*

The key goals of functionality include improving the capabilities of observation and analysis, information exchange and management of the shared situational picture. The management of disruptions and identification of information-based influencing by technical means were also highlighted.

The pace of changes in the operating environment requires constant development of national observation and analysis capabilities in cooperation between companies and authorities. Advanced observation and analysis capabilities allow for timely and informed decision-making. In the future, the observation and analysis capabilities should be based on extensive datasets and targeted analysis supported by machine learning. The technical capability of companies and authorities to detect and prevent data security threats, in particular, needs development. The aim is to make sharing the situational picture faster and automate responses to cyber threats.



As part of the promotion of functionality, there is a need to develop a common information exchange and observation platform where the common situational picture can be managed. Critical parties should have current and essential information about the current situation relevant to their own activities. Furthermore, the situational picture should include an estimate of the future, i.e. data to support foresight. The aim of the platform is to enable the change in the operating environment where different parties can exchange information confidentially. In addition to the observation platform, building channels to allow for quick communications from different sectors is being planned.

By developing the management of disruptions, the recovery of organisations from data security deviances can be accelerated. The national disruption management capability should be based on cooperation, networks and shared operating models. The programme includes a preliminary measure of increasing cooperation between commercial and official security operations centres in the event of an extensive cyber disruption.





As information-based influencing increases, ensuring the reliability and integrity of information becomes increasingly important. Methods and tools for identifying and preventing information-based influencing are being developed in the programme. An additional goal is to provide authorities with the technical ability to detect phenomena aimed at information-based influencing through social and digital media.

## Cooperation networks

*The key objectives of the priority are the development of cooperation models and increased influence in international cooperation. National cooperation and pool activities will also be developed.*

The cooperation models for disruptions should be implemented in cooperation between companies and authorities. In practice, this means e.g. establishing common operating principles and protocols for addressing different needs, sharing best practices and creating models in order to respond to targeted attacks. Different operating models and methods of different companies and authorities will be coordinated.

In the context of international influencing, more cooperation with the authorities in charge of the security of supply of the EU and Sweden, for example, is required in order to allow for international cooperation in preparedness measures, access to the latest research data and situational awareness as well as influencing the content of development.

Increasing international cooperation requires further specification of the roles and goals of authorities.

In addition to cooperation models and internationalisation, national cooperation and pool activities must also be developed. Cooperation should be cross-sectoral and a natural part of the organisations' activity. The possible methods include improving the activities of the sectors' confidential Information Sharing and Analysis Centres (ISAC), development of the National Cyber Security Centre's sector-specific services and supporting pool committees in identifying new cyber projects and preparing project proposals.

## The future

*The priority of the future refers to the study of rising phenomena relevant to the area in cooperation with the research community both nationally and internationally.*

The objective is to improve preparedness for cyber risks posed by new phenomena. The aim is to generate data about the risks posed by rising phenomena relevant to security of supply and digital security through cooperation with the research community. In practice, cooperation with the research community could mean using developing technologies in exercises or studying international indicators of digital security. An additional goal is to secure critical national data security expertise, e.g. by expanding both national and international education cooperation and strengthening cryptography-related expertise.

## PART 5: PROGRAMME IMPACT

**The impact of the programme refers to the development in the digital security of Finnish society gained through the programme. The programme is limited to ensuring security of supply, but there can be a broader positive impact on the cyber security of society through the initiation of new activities and investments and stronger cooperation structures.**

The aim is to have the effects of the programme reach wider than the projects carried out as part of the programme. The projects encourage companies and organisations that form developing communities with their own methods to take part in the activities. The tools that support the activities will prove to be useful, be applied extensively and developed independently.

Overall, the programme launches new solutions and encourages their use. Through the projects carried out, companies

are supported in establishing sustainable cooperation structures and operating methods as well as nationally viable business and networks where companies and authorities can work together. The projects of the programme yield long-term benefits for security of supply, e.g. by initiating activities on market terms that support security of supply. In order for the programme to succeed, strong commitment to the goals and implementation of the programme and applying the results is required from companies.



# APPENDIX 1. **FRAMEWORK AND PRIORITY OF THE PROGRAMME'S PROJECTS**

The projects selected to the programme must improve the security of supply of as many parties that manage society's critical infrastructure as possible. An additional requirement is that the law does not oblige parties critical to security of supply that benefit from the results of the project to fund the presented preparedness actions at their own expense. The results of projects must be relevant to the security of supply of society as a whole and the safety of the public, and it must be impossible to achieve the desired level of security of supply or safety on market terms quickly enough.

The funding of projects complies with the principles of state aid legislation without causing any distortion of competition. An advantage here is to have a public organisation or a (nationally) relevant party in charge of the project or as the procurement organisation of the project. In order to receive funds from the National Emergency Supply Agency, the funds applied for must only be used to cover the additional expenses generated by implementing the required additional level of safety. The project can receive funds from other parties and have various other objectives. However, the additional objectives cannot be in conflict with the goals of the National Emergency Supply Agency and the National Emergency Supply Agency shall only provide funds aimed at accomplishing its own goals.

The following criteria are also used as the basis for selecting and, if necessary, prioritising the projects:

- Supports the business continuity management of critical companies
- Supports the continuity management of critical sectors
- Promotes cooperation between authorities and companies
- Develops common structures and operating methods of the sector
- Is a (joint) exercise related to preparedness
- preparedness measures that improve the crisis tolerance and operating reliability of critical (digital) infrastructure
- Improves material preparedness
- Supports the analysis and follow-up of security of supply's situational picture
- Generates viable business that will survive without the National Emergency Supply Agency's funding in the future (developing ecosystem)
- Has long-term effects
- The ownership, further development and management of the results of the project are known when the project is initiated (commitment of and support from stakeholders)
- Statement from a ministry relevant to the administrative branch that supports the project





# PARTIES IN CHARGE OF THE PROGRAMME

**The National Emergency Supply Agency (NESA)** is an organisation operating under the Ministry of Economic Affairs and Employment. It is tasked with planning and operative measures related to developing and maintaining security of supply. The National Emergency Supply Agency is responsible for the planning, coordination, funding decisions and project portfolio management of the Digital Security 2030 programme in cooperation with its stakeholders.

**The National Cyber Security Centre of the Finnish Transport and Communications Agency Traficom** develops and oversees the operating reliability and safety of communication networks and services and provides a situational picture of data security. The National Cyber Security Centre is a key partner of the National Emergency Supply Agency in planning the Digital Security 2030 programme and achieving its goals in practice.

The role of **the Digital Pool** and the organisations involved in its activities in the programme is to provide advice and support the activities of the programme. The company groups of the Digital Pool prepare project templates for the National Emergency Supply Agency's programme and support putting the results into practice in the operations of companies critical to security of supply. The results are also used in preparing new projects that complement the programme.

**Other stakeholders** participate in planning the programme and achieving the goals in practice through projects and separately specified guidance roles. These stakeholders include, for example:

- **sector-specific pools of the National Emergency Supply Organisation** that contribute to the selection, development and implementation of digital security preparedness measures in their respective sectors
- **companies** that participate in the specification of needs related to digital security, the projects of the programme and putting the results of the projects into action in their own activities. In addition, many companies are in charge of projects when such parties are sought through procurements made as purchased services.
- **authorities** that take part in ensuring digital security in sectors critical to security of supply
- **educational institutions** that carry out research and teaching related to digital security or development that supports companies
- **organisations** that advance digital security





**HUOLTOVARMUUSKESKUS**  
FÖRSÖRJNINGSBEREDSKAPSCENTRALEN  
NATIONAL EMERGENCY SUPPLY AGENCY