



Lessons learned from Ukraine regarding Finland's security of supply



Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency



Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency

www.huoltovarmuuskeskus.fi

Security of supply refers to safeguarding the economic functions, the production and availability of essential goods, materials and services, and the critical infrastructure necessary for the livelihood and protection of the population, the national economy, national defence and security, both during and in preparation for serious disruptions under normal conditions and during emergency conditions.

The National Emergency Supply Agency (NESA) is a government agency that supports public authorities, businesses and organisations in maintaining and developing security of supply. It also plans and implements preparedness measures designed to safeguard security of supply.

Publisher: National Emergency Supply Agency (NESA)

ISBN: 978-952-7470-53-4

Cover photo: Jarna Hartikainen

Layout: KMG Turku

Year of publication: 2026



Table of contents

Summary	1
Ten key lessons learned	2
Introduction	4
Different stages and different measures, but the same direction	5
Development of the war in Ukraine	5
SUUNTA planning framework	6
The 360° preparedness model – comprehensive management, domain by domain	8
Cooperation between the government and companies as a means of ensuring continuity	8
Strong cooperation between the central government and companies	10
Energy supply	11
Digital security	12
Logistics	12
Physical security	13
Finances	13
Information security	13
Materials	14
Personnel and the general public	14
Key dependencies	16
Conclusions	17

Summary

At the time of writing, Russia's invasion of Ukraine has been going on for four and a half years. During this time, the National Emergency Supply Agency (NESA) has undertaken several trips to Ukraine to gain experience and develop Finland's security of supply in preparation for serious disruptions and potential military conflicts affecting society as a whole. Ukraine's experiences show that a society's ability to function during a serious and protracted crisis depends on its ability to maintain basic everyday functions and face the crisis as a nation acting in unison. The success of preparedness is not determined solely by the protection of any single system, but by combined efforts across the domains of energy supply, digital security, logistics, physical security, finances, information security, materials and personnel. In a protracted and serious crisis, the most important of these is personnel, meaning the people who keep the various functions of society running and their psychological resilience.

Our understanding of the targets of Russia's military operations has improved throughout the war in Ukraine. These targets include not only military sites, but, to an increasing extent, civilian targets related to security of supply, such as energy supply, telecommunications, food and water supply and logistics facilities. The lessons that the NESA has learned from Ukraine can be boiled down to the concept of **360° preparedness**, according to which every organisation seeking to safeguard their own operations should examine their preparedness in a comprehensive manner, covering the domains of digital security, energy supply, information security, physical security, finances, materials, logistics and, most importantly, the ability to function of personnel. Preparedness in each of these domains contributes to overall preparedness, both in terms of an organisation's own operations and the provision of services to other organisations.

The lessons learned from Ukraine that apply to all sectors include the decentralisation of operations, alternative operating procedures, sufficient backup power, prioritisation of critical resources, repair capabilities, protection of personnel, shared situational awareness and close cooperation between the public and private sectors. The continued functioning of the economy also contributes to security of supply: the cash flow, payment transactions, insurance and funding of companies enable the provision of critical services.

During the use of military force, the focus of operations and the exertion of influence shift gradually between different stages as the situation develops, both at the societal level and in terms of individual organisations. The **prevention** stage involves building credible, operator-specific and joint preparedness and deterrence, as well as confidence in capabilities and agreements. In the **crisis** stage, personnel are protected and prepared, shared situational awareness is established and communicated, command is ensured, readiness is enhanced and the implementation of preparedness measures is initiated. In the **serious disruption** stage, measures are prioritised, alternative procedures are implemented and quick repairs are initiated. The **escalation** stage involves preparing for recurring damage and the depletion of resources. In the **protraction** stage, the key priorities are the renewal of personnel, finances and production capacity, as well as ensuring that society can cope. Finally, the **adaptation and normalisation** stage is not just about rebuilding what was lost, but also about strengthening future operations and operational reliability.

This report summarises the key findings relating to lessons learned about Ukraine's security of supply, so that all organisations can take them into account and apply them as part of their own efforts to identify and, where necessary, develop preparedness measures, including through closer cooperation with stakeholders.

Ten key lessons learned

1. The objective: Keep everyday life as normal as possible

The continuity of work, education, training, trade and services sustains the economy, strengthens the population's ability to function and builds confidence in the future. The aim is not to maintain complete normality, but to ensure that society's basic functions continue to operate adequately under the changed circumstances. This provides the public with a clear understanding of what they are fighting for. People – including the personnel of critical organisations – must also be given the opportunity to carry on with their daily lives and to recover.

2. Evolving threats: Integrate air defence into the protection of critical civilian infrastructure

Drones and deep precision strike capabilities have transformed the nature of warfare, enabling repeated and cost-effective operations even far from the front line. The systematic targeting of civilian infrastructure by air strikes and the increasing variety of the methods employed have changed the protection requirements for critical infrastructure.

In particular, the protection requirements of energy supply, logistics and telecommunications infrastructure and critical functions located in residential areas must be more effectively coordinated with national air defence planning and operations, taking their impact into account.

3. Alert capabilities: Relay information on air threats quickly via digital alert apps

The public, the authorities and the personnel of critical companies must be provided with up-to-date information on any potential drone and missile threats without delay. Prompt information about potential threats and their causes is essential to ensure that the public and critical personnel can seek shelter in a timely manner. This requires the rapid and secure sharing of information, reliable digital communication links, alert applications tailored to this specific purpose and backup arrangements for communication.

It is important for society to not shut down completely in the event of an air threat, which

is why protective measures should be risk-based, enabling critical functions to continue as effectively as possible. Operating procedures for dealing with alarm situations may vary depending on the region, organisation, establishment and work tasks, so alternative operating models must be identified in advance. It is also essential to design systems in such a way that they do not merely issue alerts, but also enable citizens to form an adequate situational picture from their own perspective. In Ukraine, this is also supported through the utilisation of existing discussion platforms.

4. Situational awareness: The situational picture is a shared operational resource

Up-to-date information on threats, the actual impact of disruptions, repair needs and available resources enables organisations to protect themselves, take corrective action and prioritise their resources and time. Information must flow in both directions between the authorities, companies and the public.

A shared situational picture does not mean that all information is shared with everyone, but rather that each operator is provided with relevant and sufficient information for their tasks at the right time to support their decision-making.

5. Prioritisation capabilities: Develop a common prioritisation model

Company-specific, market-based prioritisation is the primary approach and should also be permitted to some extent during government intervention. A common, society-wide prioritisation model is needed e.g. to allocate personnel, transport services, energy, materials, protection and repair resources in situations where not everything deemed critical or important can be protected or restored simultaneously and the use of resources needs to be prioritised based on societal and security of supply needs.

The common principles and operating models for prioritisation must be agreed upon in advance so that the model facilitates situation-specific solutions. Applying the same principles may lead to different outcomes depending on the situation, the area and the impacts.

6. Tolerance to disruptions: Prepare for long-term disruptions to critical dependencies

Critical functions must be able to continue operating even when the energy supply, telecommunications, material or logistics services that they require are disrupted for an extended period.

For example, backup power should be designed for key sites with a view to power cuts lasting several weeks and occurring repeatedly. At the same time, fuel, maintenance and spare parts supply chains should be secured, and manual contingency procedures and controlled recovery should be practised.

7. Decentralisation: Decentralise critical functions and strengthen alternative solutions

The conditions for the decentralisation of functions, information, warehouses, production, communications and repair resources are established under normal conditions. Critical materials and spare parts should be linked to multiple alternative or domestic production capacities, production reserves, supply channels and framework agreements.

Decentralisation reduces the significance of individual points of failure and may also make it less attractive for the enemy to target specific sites, as damaging a single site will not have a significant overall impact. In the event of serious disruptions to transport, alternative routes, terminals and arrangements for receiving international aid are required.

8. Repair capabilities: Repairing damage is a continuous process

In a protracted crisis, damaged infrastructure is not repaired just once, but multiple times, which requires the capability to repair simultaneous and recurring damage. Ensuring quick repair capabilities requires adopting design, permit, procurement and decision-making processes within companies, between companies and in relation to the authorities that are more relaxed, shorter and less costly than the ones used under normal circumstances.

Modular solutions, required spare parts, repair units, skilled personnel, equipment and the principles of protection and prioritisation should be identified in advance. Speed stems from choices made before the crisis. International aid and support are also crucial when it comes to materials, so the relevant operating models must be established in advance.

9. Government guidance and direction: Select a combination of market-based solutions and government intervention appropriate to the situation

A functioning market also helps to safeguard security of supply in the event of disruptions through alternative solutions and competition. Because of this, increased regulation or government intervention is not always the most effective solution in a crisis. Operations can also be streamlined by removing or temporarily relaxing regulations, permit procedures and other obligations that restrict or slow down market activity. It is appropriate to incorporate derogation clauses into special legislation in advance, where possible, even if legislative amendments need to be made as the crisis progresses.

Government intervention is needed especially to prioritise critical resources and in situations where the market is unable to safeguard essential functions on its own. Outside of these cases, companies operating in the market must be given the space to develop alternative solutions quickly in order to meet demand. Instead of full government control or a completely hands-off approach, the most appropriate solution may be limited government intervention that leaves implementation primarily up to the market.

Regional cooperation and intervention are particularly important during serious and widespread crises. It does not make sense to centralise all government guidance and direction, coordination and prioritisation in the capital; instead, it is important to devolve responsibility to individual regions, so that they can respond swiftly to regional and varying needs.

10. Ability to function of personnel: Ensure the availability and long-term ability to function of personnel

Organisations need personnel reserves, substitutes, multi-skilled personnel, fast-track training pathways, protective equipment, backup communication links and safe transport and communication arrangements. In a protracted crisis, the importance of personnel recovery, the sustainable organisation of shifts and long-term psychosocial support also increases.

The ability to function of personnel also depends on the safety of their loved ones and the continuity of their everyday lives. For this reason, support for personnel cannot be limited solely to arrangements implemented in the workplace.

Introduction

The National Emergency Supply Agency (NESA) engages in cooperation with public authorities and critical companies in Ukraine with the aim of sharing preparedness practices and lessons learned between countries, thereby developing overall preparedness, particularly in preparation for potential military conflicts. The aim of this public summary report is to widely disseminate the general lessons learned from Ukraine to various organisations, with a view to developing Finland's security of supply and preparedness. It is important to note that many of the preparedness measures described in this report are also relevant to other disruptions besides military conflicts.

This report is based especially on lessons learned from three study visits to Ukraine,

which involved examining energy supply and digital infrastructure, logistics, repair construction and food and water supply. The participants of the visits included the NESA's own specialists as well as representatives of other Finnish authorities and companies critical to security of supply. The report brings together the observations and lessons learned by all participants during the trip and shares them for the benefit of Finnish organisations in developing their preparedness.

Most of the lessons described in this report are not sector-specific, meaning that they are broadly applicable to the development of preparedness. In particular, there are areas for improvement relating to personnel and resilience against intersectoral dependencies that all stakeholders can capitalise on.

In addition to being summarised in the list of key lessons presented above, the findings from Ukraine are examined in this report through two complementary perspectives:

- The progression of a crisis is described using the NESA's SUUNTA planning framework, which was previously utilised in the military conflict scenario published by the NESA in spring 2026. The framework divides crises into the following stages: prevention; crisis 0–3 months; serious disruption 3–6 months; escalation 6 months–1 year; protracted disruption over a year; and adaptation and normalisation.
- The 360° preparedness model outlines the domains in which all organisations should be prepared for disruptions: energy supply, digital security, logistics, physical security, finances, information security, materials and personnel.

The timeline used in this report is merely an analytical framework. An actual crisis does not unfold in such a linear fashion: different regions, sectors and organisations may be at different stages of the crisis at the same time, and the situation may also rapidly escalate and vary in intensity. What the timeline exemplifies, however, is people's ability to cope with unexpected situations: initially, pre-prepared and planned measures are the most useful, and as the crisis drags on, it becomes possible to develop new approaches and adapt to the situation. The timeline is aimed at supporting the planning and preparation of preparedness measures, thereby speeding up their application and

adaptation in a protracted crisis. The end of the report also includes an analysis of interdependencies between sectors that have repeatedly emerged in various contexts.

It is important to note that this report does not describe the preparedness of any individual Finnish or Ukrainian operator, nor does it contain any detailed information on sites, capabilities, defences or vulnerabilities. Furthermore, not all of the solutions that have proven effective in Ukraine can be transplanted to Finland as is. Instead, they must be assessed from the perspective of Finland's geography, population, market structure, legislation, technical systems and alliances.

Different stages and different measures, but the same direction

Preparedness operations and the range of measures available change as a crisis – including a war – develops. Preparations for disruptions and emergencies are mainly carried out in advance, and when successful, they also serve as a deterrence that may help prevent a crisis from arising. Once a crisis has begun, successful preparedness management involves implementing or activating the measures that were planned and prepared in advance as the situation develops, and applying them flexibly as the situation demands. No two crises or disruptions are the same. That being said, experiences and models of previous crises and disruptions contribute to a comprehensive understanding of the necessary capabilities and preparedness measures. For this report, the stages of the war in Ukraine and the development of preparedness measures were modelled with the help of the SUUNTA planning framework for security of supply, which supports security of supply and preparedness planning.

Development of the war in Ukraine

The large-scale invasion launched by Russia in February 2022 rapidly and comprehensively changed the operating environment in Ukraine. The effects of the war have not been confined solely to the front line, but have instead impacted the functioning of society as a whole: the population, companies, energy supply and telecommunications systems, transport, food supply, water supply, public services and the economy. The findings from the NESA's 2025–2026 study visits to Ukraine illustrate how Ukraine has shifted from the surprise and improvised responses in the early stages of the invasion towards the systematic management of a protracted war, continuous adaptation and reconstruction.

Even before the February 2022 invasion, Ukraine had experience of Russian interference dating back to 2014, and had made preparations especially for cyber threats. Despite this, the large-scale attack took Ukrainian society, companies and a large proportion of the population by surprise with its intensity and scale. The first few weeks were characterised by personnel evacuations and mobilisation, the breakdown of chains of command and communication, the withdrawal of foreign service providers and disruptions to supply and transport chains. Conventional operating procedures did not work in every respect, which is why manual procedures and temporary solutions had to be rapidly introduced to maintain security, service continuity, payment transactions and infrastructure.

When large-scale war broke out in the winter of 2022, companies, local communities and individuals played a key role in ensuring business continuity. Regulations and border crossing formalities were relaxed to ensure that essential goods, fuels and international aid could reach their destinations. At the same time, common criticality classifications and prioritisation principles were established, enabling scarce resources to be allocated to the most important functions. Efforts have been made to formalise these as the war has dragged on, and this work is still ongoing. To safeguard telecommunications, national roaming, satellite connections and alternative communications solutions were rapidly introduced. In the transport and logistics sectors, disruptions to air and sea transport were compensated for through the utilisation of road, rail and river routes.

As the war dragged on and the front lines became more or less static, strikes on critical civilian infrastructure behind the front lines became systematic and recurrent. Energy supply, telecommunications, transport, fuel, food and water supply systems have been subjected to constant physical attacks, cyber influence activities and sabotage. Drones and missiles make it possible to reach targets far from the front line, and the same systems can be targeted multiple times, both during and after repairs. Consequently, the focus of preparedness has shifted from repairing individual instances of damage to the ability to withstand, contain and repair multiple and recurring instances of damage.

Based on Ukraine's experiences, the protection of critical infrastructure cannot be based solely on the technical reinforcement of individual sites. Instead, it requires protection coordinated with air defence, decentralisation of operations, alternative connections, backup power, decentralised warehouses, modular solutions and rapidly deployable repair resources, along with verified information on air and other threats that can be relayed quickly. The ability of the public, the authorities and companies to protect themselves depends on warning information and situation-specific instructions being made available without delay via digital alert services, and on there being effective backup arrangements in place for communications.

During the protracted war, the challenges have gradually shifted from managing immediate destruction to conserving resources and maintaining the functioning of society. The operations of companies are affected by personnel shortages, mobilisation, population shifts, the availability of skilled personnel, the psychosocial

strain and lack of sleep of personnel and the availability of spare parts, fuels and repair equipment. Personnel shortages have been addressed by methods such as training personnel for new roles, increasing multi-skilling and automation and strengthening the position of women in previously male-dominated jobs. At the same time, cooperation between companies, the authorities and international operators has evolved from the improvisation carried out in the initial phase into more systematic contract, funding, logistics and management arrangements.

During the NESA's study trips to Ukraine, everyday life continued seemingly as normal in many areas, despite the attacks, air-raid alerts and power cuts. Workplaces, schools, shops and services continued to operate, even though they had to constantly adapt their operations. In this context, normal everyday life does not mean that the effects of war are absent. Instead, it manifests as actively maintained crisis resilience and perseverance. As a result, community cohesion, family and the need for connection are emphasised in particular. The continuation of economic activity, exports, payment transactions and markets generates resources for defence and reconstruction and strengthens the population's ability to function and their confidence in the future.

Adaptation does not mean a return to the situation that existed before the war. When it comes to reconstruction, the aim has been to build systems that are more decentralised, better protected and easier to repair than before, as well as, in some respects, cheaper. Production facilities and warehouses have been relocated, transport routes have been diversified and companies' own energy, communications and repair capabilities have been strengthened. The aim has been to rebuild

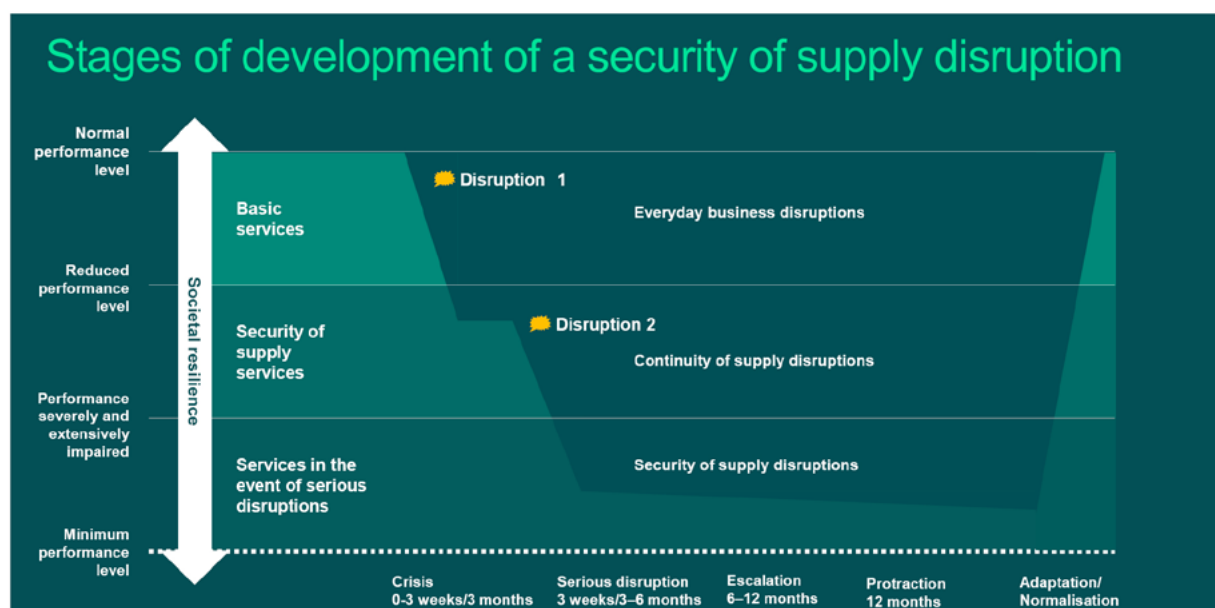
better, so that the reconstruction does not reintroduce the same vulnerabilities that the war has exposed.

Ukraine's development has not been straightforward, nor has it been the same across all regions or sectors. An individual region or system may be experiencing an acute disruption at the same time as another has already adapted and a third has moved on to the reconstruction phase. Even operations that appear to have returned to normal may quickly revert to a state of serious disruption following a new attack.

SUUNTA planning framework

In its comprehensive planning of preparedness measures, the NESA utilises the SUUNTA planning framework (Figure 1), which takes into account not only the severity of a disruption, but also its duration. The model is not organisation-specific, as it is designed to support all operators in the comprehensive and wide-ranging planning of disruption response. The six stages of the model – prevention; crisis; serious disruption; escalation; protraction; and adaptation and normalisation – describe different operating environments in society and the solutions required in each. However, the stages do not simply form a timeline progressing in a single direction; rather, they may overlap, recur and manifest in different ways across different sectors. In the following sections, the findings from Ukraine and the lessons Finland can learn from them are structured using this multi-stage model and, subsequently, further refined by sector based on the domains of the 360° preparedness model. Although the durations described in the framework are only indicative, they describe the ability of people and the market to respond and adapt in different stages.

Figure 1: The SUUNTA planning framework for security of supply



The preparedness and readiness of society is primarily based on the independent preparedness of critical operators. For companies, this means business-driven preparedness. As a general rule, companies can cope on their own with disruptions that only affect their own business operations. To help with their independent preparedness, companies can make use of basic security of supply services. Disruptions that companies cannot cope with on their own and that affect multiple operators typically constitute continuity of supply incidents, the management of which requires collaborative, market-based solutions. Incidents that pose a broader threat to the functioning of society and the livelihoods of the population and cannot be resolved by the market alone require security of supply services provided by the central government and related government capabilities.

The early stages of a disruption are characterised by uncertainty and a sense of being out of control. As the situation escalates, adaptation begins, and operating models become increasingly clear and understandable. In a protracted situation, a whole new set of established operating methods emerge, and new market solutions based on business considerations begin to mitigate the situation.

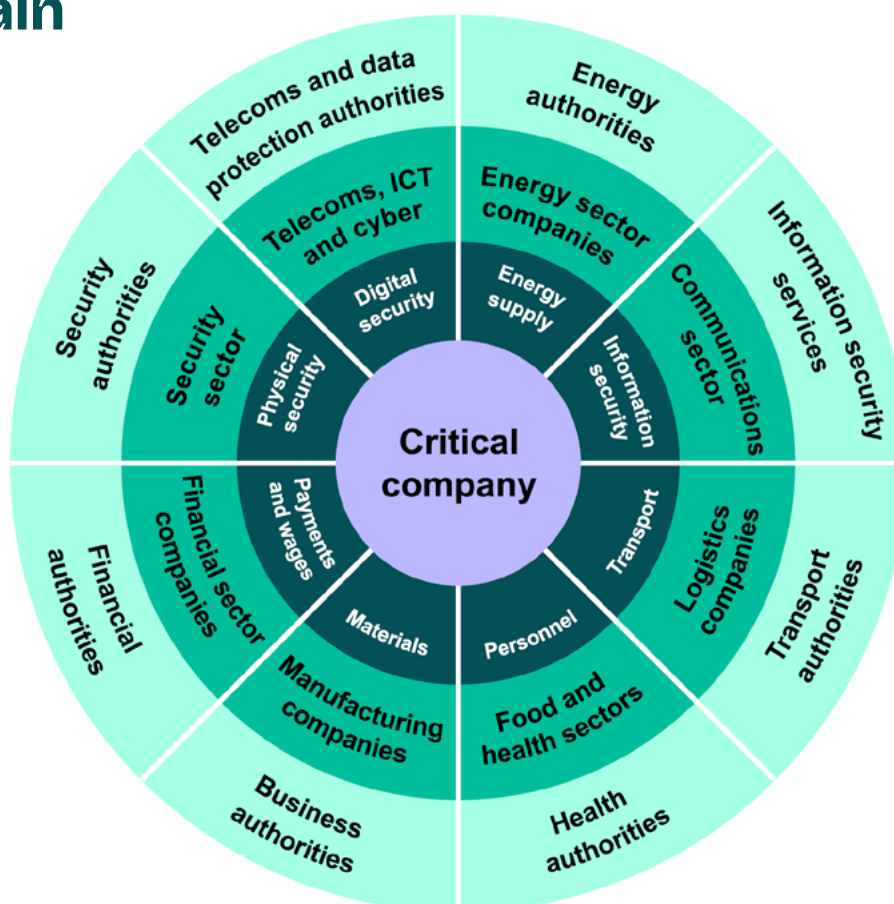
In line with the observations made in Ukraine and the lessons learned from them, the focus of preparedness measures shifts gradually as the situation develops. Although every crisis unfolds in its own way, certain common characteristics can be identified. In the prevention stage, it is possible to establish credible preparedness, cooperation frameworks, a shared situational

awareness model, agreements and a material basis, which can then be leveraged rapidly in the event of a disruption. In the crisis stage, hostile influence operations typically take the form of information influence activities, sabotage and cyber influencing, as well as limited and disputable operations. At this stage, it is often difficult to identify the actual party behind these operations, or their involvement may be disputed. During the crisis stage, personnel and critical resources are protected, readiness is enhanced, command and control is ensured and international cooperation mechanisms are activated. In the serious disruption stage, the aforementioned hostile operations are supplemented by deep precision strikes using drones and missiles as well as limited military operations. This stage involves prioritising services, adopting alternative operating procedures and initiating quick repairs. At this stage, it is often easy to identify and difficult to dispute the party behind the disruption. In the escalation stage, in addition to acts of sabotage and deep precision strikes, one must be prepared to withstand large-scale military operations and prepare for repeated damage, the depletion of resources and the relocation of operations. If the disruption continues for over a year and turns into a war of attrition, it has entered the protraction stage, at which point personnel coping, funding, production capacity and the renewal of supply chains become crucial. Finally, in the adaptation and normalisation stage, the aim is not merely to restore the status quo, but to build systems that are more decentralised, more resilient and more repairable than before.

Table 1. Preparedness measures identified from the lessons learned in Ukraine across different time horizons

Stage	Time span	Main focus of preparedness
Prevention	before the crisis	Identifying criticalities, responsibilities and decision-making authority, agreements and contracts, personnel and vehicle reserves, exercises, decentralisation and decentralisation plans, warehouses, backup power and backup power plans, repair capabilities and secure information exchange.
Crisis	0–3 months	Enhancing readiness, supporting personnel and their families, protective measures, decentralising warehouses and equipment, deploying backup connections, proactive communication and safeguarding cash management.
Serious disruption	3–6 months	Prioritising services and materials, alternative routes and operating methods, manual contingency procedures, quick repairs, preparing and initiating exceptional procurements, identifying domestic production requirements.
Escalation	6 months–1 year	Withstanding recurring disruptions, recycling repair resources, flexible supply chain maintenance, replenishing stocks, relocating production and services, continuously adapting physical and digital protection measures, launching domestic crisis production.
Protraction	over 1 year	Personnel coping and renewal, rapid training, continuity of investments and funding, strengthening domestic production, equipment lifecycle management and sustainable planning of service levels.
Adaptation and normalisation	as the situation stabilises	Prioritising recovery, rebuilding in a more resilient manner than before, controlled dismantling of temporary solutions, evaluating lessons learned, replenishing stocks and renewing preparedness.

The 360° preparedness model – comprehensive management, domain by domain



From the perspective of an individual company, preparedness is all about comprehensive management. This means that it is important to examine how different factors influence one another and to identify key stakeholders. Identifying operational dependencies and critical supply chains helps with the preparation of risk assessments and the most critical risk management measures, thereby contributing to comprehensive 360° preparedness.

The domains that all organisations, regardless of their sector, must take into account in their preparedness are energy supply, digital security, physical security, logistics and materials, as well as information security – which is becoming increasingly crucial – and, most importantly, the ability to function of personnel. By taking all of these domains into account, organisations can ensure that there are more elements supporting their business continuity than there are potential chain reactions threatening it.

Identifying the key prerequisites for business continuity helps organisations to identify the parties that influence their operations: the companies in their supply chains and the authorities responsible for regulation, sectoral guidance and maintaining situational awareness. These parties constitute a network which, through smooth cooperation, can identify effective response models for disruptions that take into account different perspectives across the entire supply chain and society as a whole.

Cooperation between the government and companies as a means of ensuring continuity

Ukraine's experiences highlight that the independent efforts of critical companies and the capabilities of public authorities complement one another. In Ukraine, efforts to establish cooperation and information exchange between the authorities and companies began only after the Russian invasion, as prior to this such preparedness cooperation and related models

were virtually non-existent. The building of this cooperation in a situation where both parties are under pressure to reorganise their operations only further emphasises its significance and the importance of foresight for preparedness as a whole.

Companies must be able to protect their personnel and operations, maintain services that are critical to society, decentralise their resources and repair damage. The government, in turn, must facilitate joint prioritisation, air defence to protect the most critical targets, additional cyber security solutions for critical operations, the financial conditions for repair reconstruction during crises and the organisation and safeguarding of transport routes to facilitate logistics. This requires maintaining a continuous, daily situational picture of the impact of the war on critical functions, on the basis of which ongoing, prioritised decisions are made regarding protective measures and repairs.

- **Shared situational awareness and prioritisation:** operators need to have a common understanding of the threat situation, critical needs, available resources and the order of restoration. Apps that alert users to air threats, in turn, form a key foundation for public safety and the operations of the personnel of critical companies.

- **Protecting critical infrastructure:** companies' own physical, structural, digital and organisational security measures must be coordinated with those of public authorities and defence planning. In air defence in particular, the development and refinement of procedures become increasingly important as a war progresses.
- **Securing supply chains and international aid:** logistical hubs, responsibilities, funding, contracts, insurance, warehousing and transports must be planned and prepared in advance of a crisis to ensure rapid response.
- **Flexible regulation:** exceptional procedures relating to permits, procurement, working hours, transports, energy and communications must be defined in advance to enable a swift response in the event of a crisis.
- **Economic continuity:** exceptional tasks, high-risk operations and the maintenance of critical services require effective compensation, financing, insurance and guarantee mechanisms. Even if their operations are directed by the government, companies still need to be paid for their services in order to maintain long-term business continuity.



Strong cooperation between the central government and companies



Air defence as part of the protection of civilian infrastructure

Air defence is **essential for operations and reconstruction**: otherwise, new and repaired critical infrastructure will be destroyed.

Companies' own security measures help, but are not enough when faced with attrition tactics and massive missile and drone strikes.

Air defence must be integrated into the **protection of national civilian infrastructure**, rather than treated as a separate military issue.



Critical infrastructure is exposed to simultaneous threats

Threats materialise simultaneously: **information, kinetic (missiles, drones), sabotage, cyber, long power cuts, personnel shortages, material shortages**.

The threat level varies over time and from region to region ► security models must be **flexible and scalable**.

Technical security measures alone are not enough without operating procedures and personnel preparedness.



International aid and logistics hubs

The logistics of international aid require:

- logistics hubs to be **established in advance**
- contractual arrangements to be established during peacetime.

A disruption to logistics can also quickly paralyse other critical infrastructure.



Emergency legislation and agile regulation

Regulatory flexibility and deregulation

Speeding up procurements

Flexibility in working time and rest period regulations

Exemptions relating to transport, energy and communications

These grant companies and public authorities the **power to act in a crisis**.

Energy supply

All critical functions are dependent on the supply of energy. Energy production and distribution infrastructure has been one of the main targets of attacks in Ukraine throughout the war, as power cuts have widespread repercussions for other sectors and have a visible impact on people's everyday lives, as well as on heating during the winter. Long and frequent power cuts place a strain on backup power generators, batteries, fuel supplies, maintenance personnel and spare parts

Lessons for Finland's preparedness

- Scale backup power solutions based on the actual minimum requirements of critical services and the possibility of prolonged power cuts.
- Ensure the supply of fuels, transports, safe storage, maintenance, test runs and spare parts.
- Decentralise production and develop isolated and local generation capabilities in appropriate locations.
- Prioritise the supply and restoration of electricity in accordance with pre-agreed criteria that take into account different sectors.
- Test the preparedness of operators in the energy, telecommunications, water supply, food and logistics sectors in joint exercises.



Digital security

Telecommunications, information systems and digital identity enable the seamless flow and exchange of information, facilitating management, alerts, payments, logistics and industrial production and distribution. Simultaneous physical and cyber disruptions can eliminate both a primary system and the ability to control it.

Lessons for Finland's preparedness

- Establish alternative connections and nationally compatible backup arrangements, including satellite connections for critical applications.
- Ensure the operation and resilience of communications networks, even during power cuts, as functioning communications are essential for the flow of information and alert applications and contribute to psychological resilience by enabling people to stay in touch.
- Isolate critical environments appropriately and manage access rights and remote connections.
- Ensure that backups are recoverable, distributed and regularly tested, utilising secure data storage solutions located both within the country and abroad. Ensure that the most critical data resources are located in facilities that can withstand potential air strikes.
- Define the order of priority of services, customers and network nodes and ensure that access to services can be restricted in a controlled manner.
- Practise switching from a digital to a manual way of working, and back again.

Logistics

Logistics are essential for numerous sectors and functions, such as energy supply, food supply, water supply, healthcare, manufacturing and international aid. Finland's position as a logistical island means that the continuity of maritime links is particularly important. Maintaining logistics requires the coordination of ports, terminals, road and rail transport in all circumstances.

Lessons for Finland's preparedness

- Prepare realistic contingency plans for serious disruptions to maritime transport, and conduct exercises to practise the prioritisation of transport flows and the joint management of operations.
- Secure alternative routes, modes of transport, terminals, transshipment and critical transport equipment.
- Identify in advance the statutory regulation and authorisation procedures for the introduction of exceptional arrangements for working hours, dimensions, weights, customs and other matters relating to transport during a crisis.
- Ensure the provision of energy, information, maintenance and personnel for transport operations.
- Ensure that insurance practices for exceptional circumstances in maritime transport – which are crucial to the continuity of logistics in relation to ships or their cargo – are in place.
- Develop a common operating model for the receipt, storage, allocation and onward transport of international aid

Physical security

Physical security is a multi-layered system in which location, decentralisation, structural protection, detection, access control, reparability and special defence measures taken by the authorities, particularly against air threats, complement one another. Not everything can be protected to the same degree.

Lessons for Finland's preparedness

- Assess and classify critical assets and functions in accordance with harmonised principles and update their classification as the threat evolves.
- Decentralise operations and eliminate individual points of failure even under normal conditions.
- Draw up sufficient building plans relating to protection measures and have operators procure the materials required for their implementation in advance.
- Ensure that permit issues relating to critical civil infrastructure or the slow speed of the permit process do not become obstacles to the construction of protective structures.
- Wherever possible, make use of underground construction in advance, as this is the most effective way of protecting the most critical sites.
- Procure modular and portable protective structures that can be quickly installed and scaled during repair construction in advance for critical sites.
- Plan the safety of repair personnel during work in hazardous areas.
- Integrate the security needs of critical civilian infrastructure more effectively into joint planning between the authorities and the Finnish Defence Forces.

Finances

Payment transactions, financing, insurance and the cash flow of companies are essential for business continuity. A critical service cannot be sustained for long based on a sense of duty alone if the associated costs, risks and charges cannot be managed.

Lessons for Finland's preparedness

- Ensure that contingency procedures are in place for payment transactions, payroll, invoicing and cash management.
- Agree in advance how exceptional service requests from the authorities are to be placed, verified and reimbursed.
- Develop insurance and guarantee models for transport, investments, repairs and high-risk activities.
- Safeguard the working capital and continuity of funding of critical companies in the event of a serious disruption.
- Assess financial dependencies as part of regular business continuity planning, not only once a crisis has begun

Information security

Reliable information reduces uncertainty and enables timely protection. In a fast-paced information environment, problems are caused not only by a lack of information, but also by conflicting, outdated or deliberately misleading information.

Lessons for Finland's preparedness

- Define a common minimum situational picture for information influence activities across sectors, as well as information ownership, distribution channels and security levels.
- Establish a two-way exchange of information: companies provide information on disruptions, while the authorities share threat and situational information necessary for operational purposes.
- Ensure that warnings, instructions and information on services are provided to the public through multiple channels.
- Hold exercises to practise verifying information, handling contradictions and communicating in situations where not all information can be made public.
- Keep critical documentation accessible, up to date and, where necessary, geographically distributed.

Materials

In a protracted crisis, resources such as spare parts, generators, batteries, protective equipment, pumps, specialised machinery and building materials are used up quickly. As regards basic building materials, production may be able to keep up with demand, but delivery times for spare parts and specialised components become extremely long. Centralised warehouses can become both logistical bottlenecks and single points of failure.

Lessons for Finland's preparedness

- Determine critical materials, consumption rates, substitute products and minimum stock levels for each sector.
- Increase the buffer stocks held by companies and operators by shifting from a 'Just in Time' approach to a 'Just in Case' approach.
- Decentralise warehouses based on points of use, transportability and security.
- Integrate warehousing with domestic production capacity, production reserves, maintenance and international procurement and support channels.
- Plan the prioritisation, allocation and replenishment of materials in the event of multiple simultaneous incidents of damage.
- Where appropriate, give preference to modular and standardised solutions that can be used at several sites.

Personnel and the general public

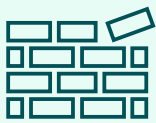
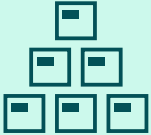
It is ultimately up to personnel whether plans are put into action. In Ukraine, the availability of personnel has been reduced by mobilisation, evacuations, emigration, injuries, deaths and prolonged stress. It should also be noted that critical tasks require a greater level of competence, flexibility and personal risk-taking than usual.

When it comes to personnel and the general public, it is essential to ensure access to clean food and water – if there is no clean water, personnel and residents will leave, and when the water supply is restored, they will return. Food supply is also an important consideration for organisations because there may be temporary delays and disruptions in food logistics. When it comes to safeguarding food supply, the same principles apply as in the preparedness of any organisation: backup power solutions are necessary, communications must function properly and operations must be decentralised.

It is worth noting that, despite attempts to undermine it, the food supply system in Ukraine has functioned exceptionally well overall throughout the war. Good food has become one of the cornerstones of mental resilience.

Lessons for Finland's preparedness

- Identify critical tasks, key personnel, substitutes and the need for rapid employee onboarding.
- Coordinate compulsory military service, personnel reserves and the personnel needs of critical civilian functions.
- Ensure personnel safety, mobility, first aid, rest and communication, as well as shelters.
- Focus on providing guidance and training on self-preparedness for the public, as well as on ensuring accessibility.
- Draw up plans for support for personnel and, where necessary, their families, as well as for evacuation, accommodation, psychosocial support and financial incentives.
- Expand the pool of skilled personnel, increase multi-skilling and establish fast-track training pathways.

Domain	Summary
Energy 	• Critical functions must be able to withstand prolonged and recurring power cuts. Backup generators are essential, but alternative sources of backup power should also be assessed: batteries, solar power, wind power. • Fuel supplies and heating facilities are priority targets, and operators in various sectors must also independently prepare for potential disruptions to these services. • Electrical substations and transformers are priority targets > protecting them aboveground is extremely difficult. Decentralised and isolated generation and the appropriate placement of facilities improve resilience.
Digital security 	• Real-time information is essential for evacuations, operations and personnel safety. Communicating threats to the civilian population is a priority. Communication and situational picture platforms are a key part of psychological resilience. • Preparedness requires backup connections (satellite), remote connections, cyber defence and the decentralisation of data to the cloud and abroad. • Social media and apps are key tools.
Logistics 	• Critical transports must be prioritised, and alternative routes, modes of transport, terminals and communication links must be established for them. • Risk management must account for regional and temporal variations in threat levels. • In Finland, key considerations include Baltic Sea connections, transport insurance during emergency conditions, the supply of fuels and capacity to receive international aid
Physical security 	• Placing functions and structures underground is the most effective approach; decentralisation and redundancy are also important. • Fast, scalable and modular protection and repair solutions (containers, concrete structures, drone protection nets). Structural engineering and having operators procure protective materials in advance are also important. • The air defence needs of critical infrastructure must be integrated more effectively into national defence and preparedness planning in order to protect it from large-scale military operations.
Finances 	• Payment transactions, payroll, invoicing, cash management and funding must continue even during a crisis. • The operations of critical companies are supported by compensation, insurance and guarantee schemes agreed upon in advance. • Controlled flexibility in contracts, liabilities and payment terms.
Information security 	• Reliable, swift, consistent and harmonised provision of information. • The role of information provision in supporting psychological resilience. • Controlled utilisation of social media and digital channels. • Prevention of false information, disinformation and attempts to influence public opinion.
Materials 	• Shortages of specialised parts, spare parts, generators, protective equipment and other critical equipment can put a stop to repairs. • Warehouses must be scaled, decentralised and integrated with flexible procurement and contract models. • Domestic production capacity and international supply channels. • Modularity and standardisation speed up replenishment.
Personnel 	• Ensuring the availability, competence and ability to function of critical personnel is more important than technical solutions. • Personnel reserves, substitutes, fast-track training pathways. • Protective equipment, psychosocial support, incentives and, where necessary, support for personnel's families. • Personnel shortages must be alleviated by broadening the pool of skilled personnel and strengthening multi-skilling. • The access of personnel and the general public to food and water must be ensured. • It is also important to look after families and loved ones as far as possible, so that personnel are able to work.

Key dependencies

The domains of the 360° preparedness model cannot be developed as separate silos, as a disruption affecting any one domain can quickly undermine all the others as well. Impact chains must also be examined in reverse and as circular processes. For example, a disruption to the energy supply can impair telecommunications and logistics, which in turn makes it more difficult to deliver fuels and repair the electricity network. The aim of preparedness is to identify such self-reinforcing

cycles of disruption and break them through alternative arrangements, decentralisation, emergency stockpiles, contingency procedures and jointly agreed upon prioritisation principles.

When assessing, developing and conducting exercises relating to organisational preparedness, at least the following impact chains must be examined:

Impact chain	Practical significance
Energy ► continuity of critical sectors ► people's everyday lives	Disruptions to electrical grids and energy distribution affect business continuity across all sectors in the absence of backup power solutions and the capacity to withstand prolonged disruptions. For this reason, backup power and alternative energy solutions are crucial across all sectors.
Energy ► digital security ► situational awareness and command	Power cuts disrupt communication networks and information systems, making it more difficult to establish situational awareness, exercise command and control, issue alerts and provide information to the public. Because of this, backup connections (e.g. satellite connections) are important.
Digital security ► personnel ► ability to function and psychological resilience	Digital communication links enable the issuing of alerts and instructions and communication. Their absence undermines personnel's ability to protect themselves, make decisions regarding safety and carry out their duties. Communication helps to maintain psychological resilience.
Personnel ► repair capabilities ► energy supply, digital security and logistics	A lack of skilled personnel, substitutes, safe transport or security measures delays repairs and prolongs disruptions to other critical services.
Materials ► repair capabilities ► continuity of services	Shortages of spare parts, raw materials or specialised equipment can turn a single fault requiring repair into a long-term capacity shortfall. Because of this, it is recommended that buffer stocks be developed proactively.
Logistics ► energy and materials ► continuity of critical functions	Disruptions to transports, logistics hubs, terminals or routes prevent the delivery of fuels, spare parts, food and other critical materials, even if they are available elsewhere.
Physical security ► personnel and infrastructure ► production and service capacity	Physical interference with personnel, production facilities, warehouses, transport links or transport hubs can simultaneously undermine several domains and also prevent damage from being repaired.
Finances ► business continuity ► critical services	Disruptions to cash flow, payment transactions, insurance, guarantees or funding may result in services being suspended, even if the technical capacity, personnel and materials for them are available.
Information security ► situational awareness and trust ► decision-making	Incomplete, delayed or deliberately misleading information can lead to incorrect decisions, undermine cooperation and trust and jeopardise the appropriate allocation of resources.
Situational picture ► prioritisation ► utilisation of all resources	An incomplete situational picture may result in scarce personnel, energy, material, security and transport resources being directed to the wrong locations or arriving too late. Because of this, a shared, pre-established situational picture is essential.

Conclusions

When it comes to security of supply, a key lesson to be learned from Ukraine is that safeguarding people's everyday lives and ensuring the ability to function of organisations' personnel are of paramount importance. Furthermore, preparedness should be seen first and foremost as the ability to carry on, persevere, recover, adapt and change. Protecting and planning the protection of critical infrastructure in advance is absolutely essential, but it is not enough on its own. Society's ability to keep functioning stems from decentralised and repairable systems, skilled people, a functioning economy, the supply of materials, reliable information and logistics that bring all these elements together.

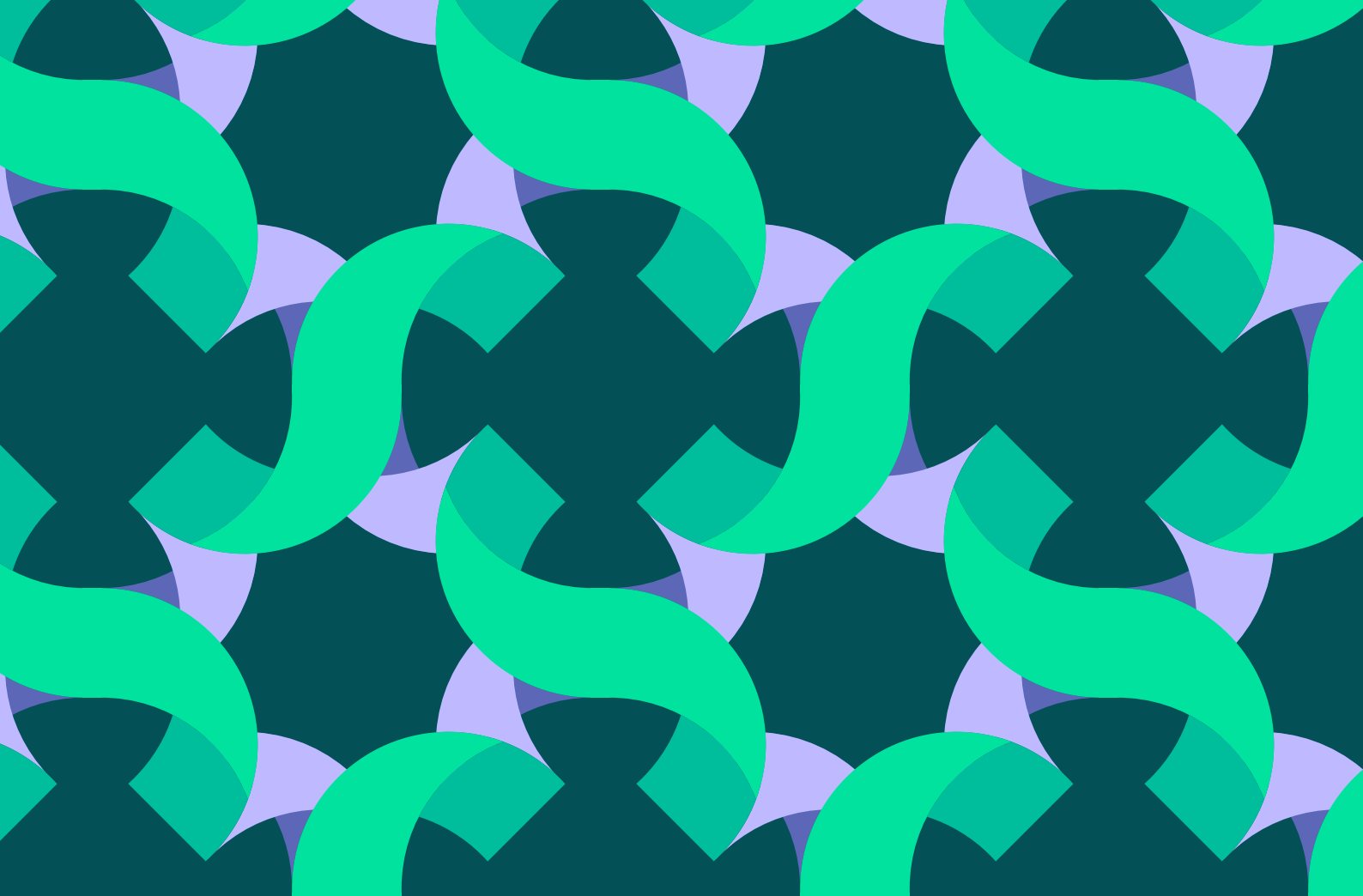
Finland's strength lies in its well-established comprehensive security model, which is based on cooperation between the public, private and third sectors. However, its effectiveness depends on its practical implementation: whether the priorities are shared, the agreements

feasible, the information shareable, the personnel available and alternative courses of action practised. When this is the case, capabilities are also established in advance, or at the very least planned, at all levels. It is also essential to ensure that citizens know how they should act. Preparedness must be at a level that makes it possible to withstand not only the first strike, but also a disruption lasting months or even years.

Effective preparedness supports prevention. It sends the message that disruption to individual targets or systems will not paralyse society as a whole, and that Finland is capable of maintaining its vital functions, support the population and renew its ability to function, even during a protracted crisis.

Keep everyday life running. Protect the people. Maintain ability to function. Security of supply is the ability to carry on.





Huoltovarmuuskus
Försörjningsberedskapscentralen
National Emergency Supply Agency