GLOBSEC
IDEAS SHAPING THE WORLD

GeoTech Center



From Comprehensive Security to Strategic Resilience: Nordic Lessons for Europe's Critical Infrastructure

Dr. Mikael Wigell

Author:

Dr. Mikael Wigell, CEO, Economic Security Forum

November 2026

GLOBSEC Geotech Center

www.globsecusfoundation.org

www.globsec.org

Disclaimer:

All of the views expressed in this piece are those of the authors and thus do not necessarily represent the official position of GLOBSEC, GLOBSEC US Foundation or associated partners

This paper was produced with financial support from the Ministry for Foreign Affairs of Sweden. GLOBSEC donors do not determine any of this paper's conclusions.

GLOBSEC
IDEAS SHAPING THE WORLD

GeoTech Center

Sweden
Sverige

Executive Summary

Finland's comprehensive security model and its security-of-supply system, as well as Sweden's total defence tradition, rest on the premise that societal functioning cannot be secured by public authorities alone. Governments, companies, municipalities and citizens all hold responsibilities for critical societal functions, organised through standing relationships and continuity planning rather than improvised in a crisis. The lesson for Europe is not that these institutions should be replicated. They grew out of unique conditions that cannot be exported as such. The question is which of the principles behind them are transferable.

This report identifies five such principles and turns them into tests against which any European arrangement can be measured: **1)** resilience is co-produced with operators, who are partners rather than consultees; **2)** trust is institutionalised through repeated interaction and backed by the state's power to require when voluntary cooperation falls short; **3)** preparedness is organised around critical societal functions rather than individual assets; **4)** mechanisms build shared capability rather than demonstrate compliance; and **5)** preparedness operates permanently, across the boundary between normal conditions and crisis. These five ask whether the logic is present. A sixth test asks whether it is resourced, i.e. whether mandates, plans, contracts and money are in place, or only cooperation. Sweden's rebuilding of total defence shows why the sixth has to be asked separately. Direction, governance and procedures came first, and capability has followed more slowly.

The report's central argument is that this logic must now be extended across borders. Infrastructure, dependencies and operators run between countries while preparedness remains national. What is needed is a regional layer organised around the functions that cross its borders. This is the shift the report describes as one **from preparedness to strategic resilience,** from absorbing and recovering from shocks to preserving freedom of action under persistent pressure. That shift rests on **governable interdependence**: dependencies that are visible, substitutable and governed in advance.

The recommendations are concrete. For the EU: regional dependency mapping for a handful of cross-border functions, access rules for the planned Cable Vessels Reserve Fleet and cable stockpiles, and resilience criteria in co-financing. For Sweden: put cross-border functions and operator networks on the agenda of the Nordic Security of Supply Network under the September 2026 Joint Nordic Declaration, and settle the status of private and foreign-owned operators in total defence through preparedness agreements and a consolidated security-of-supply law. For NATO: civil capability targets for industry, construction and financial services. For operators: map second-tier dependencies and treat recovery as a business-continuity and security matter. The report closes by proposing a two-year **Nordic-Baltic Strategic Resilience Pilot** on Baltic Sea connectivity and the northern transport corridor, tabled by Sweden in the NSSN and measured by capabilities that did not previously exist.

1. Critical Infrastructure in an Age of Strategic Pressure

Critical infrastructure protection in Europe was long approached as risk management – identify vulnerabilities, protect assets, build redundancy, prepare contingencies – and that remains indispensable. What has changed is that the continued functioning of infrastructure now shapes states' capacity to withstand pressure and preserve freedom of action.

The Baltic Sea illustrates this shift with particular clarity. The region contains dense networks of energy interconnectors, communications cables and shipping routes. In October 2023, the Balticconnector gas pipeline between Finland and Estonia was shut down after a pressure drop. Finnish investigators later traced the damage to the anchor of the Hong Kong-flagged vessel *Newnew Polar Bear,* and repairs took roughly six months.[1] On Christmas Day 2024, the EstLink 2 electricity interconnector between Finland and Estonia was severed along with four telecommunications cables. The incident was linked to the Cook Islands-flagged tanker *Eagle S,* part of Russia's sanctions-evading "shadow fleet". Repair costs were estimated at up to €60 million.[2] NATO responded by launching Baltic Sentry in January 2025, combining frigates, patrol aircraft and naval drones to monitor and deter further incidents.[3]

The legal aftermath proved as instructive as the incident. The Helsinki District Court dismissed the case against the *Eagle S* officers in October 2025 for want of jurisdiction in international waters. On 27 August 2026 the Court of Appeal reversed that ruling, holding that the offences were committed in Finland because their effects were felt there, and the defendants have applied to the Supreme Court for leave to appeal.[4] A further Helsinki–Tallinn cable was cut on 31 December 2025 by the cargo vessel *Fitburg*. On 5 November 2026 the Helsinki District Court, accepting jurisdiction on the same reasoning, convicted its captain and boatswain of aggravated sabotage (*törkeä tuhotyö*), sentenced them to three and a half years and two years and ten months respectively in prison and ordered them to pay some €1.9 million in repair and investigation costs; the judgment is not yet final.[5] These cases show how disruption to a geographically localised, often privately owned asset can rapidly become a regional, potentially international security concern.

This reflects a wider transformation of European security. Cyber operations, sabotage, economic coercion and the exploitation of supply-chain dependencies occur below the threshold of armed conflict, intended less to cause catastrophic failure than to impose costs, generate uncertainty and constrain political choices. Much resilience thinking still follows a sequence of shock, response and recovery, a logic suited to temporary, external disruption but not to persistent pressure on vulnerabilities embedded in ordinary economic relationships.

1 Offshore Energy (2024, 5 April), "With offshore repairs done, Balticconnector about to restart after six-month shut-down."
2 Braw, E. (2026, 22 April). "The shadow fleet is undermining the maritime order more brazenly than ever." Issue brief, Atlantic Council, Scowcroft Center for Strategy and Security
3 NATO (2025, 14 January), "NATO launches 'Baltic Sentry' to increase critical infrastructure security", nato.int; Supreme Headquarters Allied Powers Europe (2025, 14 January), "Baltic Sentry to enhance NATO's presence in the Baltic Sea", news release, shape.nato.int.
4 Helsingin hovioikeus (2026, 27 August). *Tiedote hovioikeuden päätöksestä ns. Eagle S -aluksen asiassa (R 16/2025/2572)* [Bulletin on the Court of Appeal's decision in the so-called Eagle S case]. Press release. https://www.tuomioistuimet.fi/ajankohtaista/tiedotteet/tiedote-hovioikeuden-paatoksesta-ns-eagle-s-aluksen-asiassa-r-16-2025-2572/.
5 Helsingin käräjäoikeus (2026, 5 November). Käräjäoikeus on antanut tuomion ns. Fitburg asiassa (R 706/2026/11841) [The District Court has given its judgment in the so-called Fitburg case]. Press release. https://www.tuomioistuimet.fi/ajankohtaista/tiedotteet/karajaoikeus-on-antanut-tuomion-ns-fitburg-asiassa/

European policy is beginning to reflect this. The EU's 2024 Niinistö report, *Safer Together*,[6] and the subsequent Preparedness Union Strategy advance whole-of-government and whole-of-society approaches and call for stronger public-private cooperation, but the institutional implications remain underdeveloped. The Niinistö report itself catalogues persistent gaps in information-sharing, regulatory flexibility and the scope of the EU's critical-entity resilience framework.[7] Finland, for its part, has argued for a horizontal, whole-of-society preparedness framework at EU level.[8] This report argues that the most valuable Nordic contribution lies not in particular institutions but in an underlying **governance logic,** and that the task is to identify which principles of that logic are transferable, and how they must be adapted to a cross-border infrastructure environment.



6 Niinistö, S. (2024). *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness.* Report by the Special Adviser to the President of the European Commission, Brussels, October 2024.

7 Niinistö (2024).

8 Ministry for Foreign Affairs of Finland, "Finland proposes EU Strategy for Preparedness Union", finlandabroad.fi; the sectoral non-papers of November 2024 remain unpublished.

2. The Nordic Governance Model: Resilience as a Shared Responsibility

The Nordic experience predates the current European debate. Its roots lie in Cold War civil preparedness and total defence, built on the premise that national security depends on maintaining critical societal functions under severe disruption. That premise matters more now that energy, telecommunications, transport, finance and much of the supporting supply chain are operated by private companies while public authorities retain regulatory and national-security responsibilities. Today, resilience is inherently a problem of coordination across institutional and societal boundaries.

Finland's comprehensive security model organises preparedness around safeguarding critical societal functions, within ordinary administration rather than a separate civil-defence apparatus. It is set out in the Security Strategy for Society and coordinated by the Security Committee, which brings ministries, authorities, business and civil society organisations under one strategic framework. The vital functions it defines are secured through strategic tasks assigned to ministries.[9] Public authorities, businesses, municipalities, organisations and citizens contribute according to their capabilities, combining statutory responsibilities with agreements, networks and voluntary cooperation. Cooperation with the private sector on security of supply runs through the National Emergency Supply Organisation, a network coordinated by the National Emergency Supply Agency (NESA) that connects authorities, industry associations and companies through standing sectoral committees, the "pools", covering the economic sectors essential to society. The committees give public authorities access to operational knowledge held by industry, and companies an understanding of the wider threat picture and their own role in it.[10]

Cross-border extensions of this model have been slower to take root. The 1992 Finland–Sweden agreement on security of supply has lapsed in practice and its structure is static. Finland–Sweden cooperation now runs through a bilateral strategic cooperation framework between NESA and its Swedish counterpart, aimed at concrete joint arrangements, and through well-established sectoral channels such as transport.[11] Nordic-level cooperation has, since 2024, been organised in the Nordic Security of Supply Network, discussed in Section 5.

Sweden's total defence rests on a related premise but has followed a different trajectory. Total-defence planning was formally resumed with the 2015 defence decision and has accelerated since 2022. Since October 2022, civil defence has been organised through preparedness sectors, each led by a sector-responsible agency, and six civil areas under county administrative boards. The Swedish Civil Defence and Resilience Agency (MCF) has coordinated the civil side since 1 January 2026, and a Cybersecurity Act transposing NIS2 has been in force since the

9 Security Committee of Finland, *Security Strategy for Society,* Government resolution, turvallisuuskomitea.fi/en/security-strategy-for-society.

10 Wigell, M., Hägglund, M., Fjäder, C., Hakala, E., Ketola, J. & Mikkola, H. (2022). *Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness.* FIIA Report 70. Finnish Institute of International Affairs; Kristeri, T. (2025). *Euroopan unionin ja Suomen taloudellisen turvallisuuden politiikan tilannekuva* [Situational report on EU and Finnish economic security policy]. Helsinki: Ulkopoliittinen instituutti/Huoltovarmuuskeskus.

11 National Emergency Supply Agency, communication to the author, October 2026.

same month.[12] Functions and industries without a sectoral home were given one in 2025, when sectors for industry, construction and trade and for foreign trade were added on the proposal of the Government inquiry on business preparedness, and a national strategy for supply preparedness for 2025–2030 followed in July 2026.[13]

The contrast with Finland is instructive: Finland organises public-private preparedness contractually, through the pools, Sweden statutorily, through sector agencies. Sweden also shows the limits of rebuilding. The National Audit Office found steering too general, funding absent in 2015–2018 and capability development gaining momentum only from 2022, and the inquiry found state-business interaction extensive but largely voluntary and insufficient.[14] Direction, governance and procedures have been delivered while implemented capability has lagged.

Norway's total-defence tradition and offshore energy focus, and Denmark's role as a maritime, energy and transport hub, add further variation. There is no single institutional "Nordic model", but a recurring governance logic in how resilience responsibilities are distributed.[15]

Five characteristics of that logic stand out as transferable. They return in Section 6 as the tests against which other European arrangements can be measured.

Co-production, not consultation. Nordic preparedness treats companies as participants before crises occur, not as entities consulted afterward. Finland's security-of-supply pools institutionalise this before disruption occurs.[16]

Institutionalised trust, not cultural trust. High societal trust helps Nordic cooperation, but attributing resilience to a trust culture would make the experience non-transferable. The useful distinction is that trust can be *institutionalised,* built through repeated interaction, exercises, continuity planning and clear information-handling rules, so that cooperation depends less on pre-existing social trust than is often assumed. Finland and Sweden show the two sides of this. In Finland, information sharing has long run through informal networks and was not legally required until recently. In Sweden, strict and divergent rules on information sharing have hampered consultation, and public-private interaction and reporting are now being made mandatory by law.[17] The Finnish model, in practice, combines the two. Institutionalised trust is therefore not only networks. It is also the state's ability to require cooperation, by contract or statute, when voluntary cooperation falls short.

Critical societal functions, not individual assets. Comprehensive-security thinking asks whether the function an installation supports can continue under disruption, recognising that functions such as electricity supply and the telecommunications, fuel, logistics and payment systems around it depend on one another in ways that rarely correspond to any single organisation.

Shared capability, not compliance alone. Regulation sets minimum standards, but trusted channels, shared situational awareness and the ability to improvise collectively cannot be regulated into existence. Nordic exercise culture treats them as capabilities to build.

Permanent preparedness, not episodic crisis management. Nordic structures operate across the boundary between normal conditions and crisis, so the actors who must cooperate in a disruption already know each other.

These characteristics matter more than any single Nordic institution. But the experience should not be romanticised. Public-private cooperation creates its own coordination problems and conflicts of interest, capacity differs between countries and sectors, and Nordic states depend on infrastructure and supply chains far beyond the region.

12 Förordning (2022:524) om statliga myndigheters beredskap [Ordinance on the preparedness of central government agencies]. Svensk författningssamling; Regeringen (2024, 17 October). Totalförsvaret 2025–2030 [Total defence 2025–2030]. Government Bill, Prop. 2024/25:34. https://www.regeringen.se/rattsliga-dokument/proposition/2024/10/prop.-20242534/; Myndigheten för civilt försvar (2025, 29 December). MSB will be Swedish Civil Defence and Resilience Agency as of January 1 2026. Press release. https://www.mcf.se/en/news/2025/december/msb-will-be-swedish-civil-defence-and-resilience-agency-as-of-januari-1-2026/; Cybersäkerhetslag (2025:1506) [Cybersecurity Act], in force 15 January 2026. Svensk författningssamling; Regeringen (2025, 9 October). Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag [Strong protection for network and information systems – a new cybersecurity act]. Government Bill, Prop. 2025/26:28. https://www.regeringen.se/rattsliga-dokument/proposition/2025/10/prop.-20252628/.

13 SOU 2024:19, *Ny beredskapssektor för industri, bygg och handel;* Government decision 19 June 2025 and SFS 2025:742, amending Förordning (2022:524); Government Offices of Sweden (2026, July), **Nationell strategi för försörjningsberedskap 2025–2030**.

14 Riksrevisionen (2025), RiR 2025:4; Swedish Agency for Defence Analysis (MTFA) (2023); SOU 2025:68, *Nya samverkansformer, modern bygg-nads- och reparationsberedskap – för ökad försörjningsberedskap.*

15 Wigell et al. (2022), *Nordic Resilience.*

16 Wigell et al. (2022), *Nordic Resilience.*

17 Ålander, M. & Boulègue, M. (2026). "War Beneath the Waves: Deterring Russian Sabotage of Undersea Infrastructure", in *War Without End: Deterring Russia's Shadow War.* Washington, DC: Center for European Policy Analysis, March 2026,

3. The Nordic Model Under Pressure: From National to Cross-Border Resilience

Nordic societies have some of Europe's most developed preparedness arrangements and are among its most interconnected. The openness, digitalisation and energy integration that support their prosperity generate dependencies national preparedness cannot manage alone.

The Baltic Sea incidents described in Section 1 make the point concretely. Redundancy kept the Balticconnector and EstLink 2 disruptions from becoming systemic failures, but repeated incidents at short intervals expose the limits of such redundancy.

The object of protection is therefore the **regional system of connectivity,** not the individual cable or pipeline. NATO's Baltic Sentry mission and closer cooperation between military surveillance, national authorities and the commercial operators who own, monitor and repair the infrastructure reflect this. The recovery chain is distributed, and no single actor controls the whole system.[18]

This also makes **recovery** a resilience question in its own right. Recovering the infrastructure and restoring the service are not the same thing. The owner recovers the asset, while the service providers that use it restore service to their customers, so the recovery chain itself runs across several companies. In the Baltic Sea incidents, that chain was carried by the operators themselves, with transmission system operators and telecommunications companies contracting and executing the repairs while the state's role was confined to investigation and surveillance, and even that role, as the *Eagle S* litigation showed, has proved contested. Subsea repair depends on specialised vessels, equipment and port access that may be scarce, commercially owned or located outside the affected country. The Balticconnector repair alone took roughly six months,[19] and in a conflict zone insurance conditions might have kept repair capacity from coming at all. The same logic extends to transformers, telecommunications equipment and control systems with long replacement times, and on land to roads, railways and power lines whose repair depends on a largely private construction industry, as Ukraine has shown. Sweden drew the conclusion in September 2026 by tasking MCF with re-establishing construction and repair preparedness.[20] Preparedness must therefore ask what capabilities are required to recover the function once infrastructure fails, who controls them, and how quickly they can be mobilised. Recovery capacity is part of infrastructure security.

Nordic energy integration shows that interdependence can itself produce resilience, as Norwegian hydropower, Swedish nuclear and hydro, Danish wind and Finland's diversified mix compensate for one another through cross-border markets and interconnectors. The objective is not independence, unrealistic for small, open economies, but interdependence whose dependencies are visible, whose alternatives are in place and whose coordination is agreed in advance.

Digitalisation pushes the challenge further. A physical operator located entirely within one Nordic country may depend on cloud services, software platforms or cybersecurity providers operating across multiple jurisdictions, with data processed elsewhere in Europe or beyond. In practice, this dependence is overwhelmingly on the platforms of three United States providers, while a large share of components and equip-

18 NATO, "Baltic Sentry", and Nordic Energy Research (2026). *Energy Security in the Nordics.* Report prepared by the Economic Security Forum for Nordic Energy Research under the Nordic Council of Ministers. Oslo, June 2026.
19 Offshore Energy (2024, 5 April).
20 SOU 2025:68; Nordic Defence Sector (2026, 2 September), "Sweden prepares to re-establish construction and repair preparedness".



ment is sourced from China. The problem becomes one of seeing the deeper technological and supply-chain relationships beneath first-order dependencies, which is where critical-infrastructure protection converges with economic security.

Financial infrastructure shows the same pattern in a sector where Nordic preparedness is less visible but no less consequential. Payments, clearing and account services are critical societal functions in nearly cashless Nordic economies, and they rest on telecommunications, electricity, cloud services and data centres that frequently sit in other jurisdictions.

Finland's security-of-supply system illustrates both the strength of Nordic preparedness and the adaptation now required. It identifies dependencies within the Finnish economy well, but many now lead outside Finland, to a Swedish logistics provider, an Estonian data connection, a United States cloud region or a Chinese component manufacturer. The next evolution of the Nordic model is therefore to **internationalise the logic of comprehensive security** by connecting preparedness networks across borders where the critical function itself depends on actors in several countries.

Finland's and Sweden's NATO accession has made a further transformation visible as infrastructure built for civilian and commercial purposes increasingly performs defence functions as well. In June 2024, the Norwegian and Swedish prime ministers and the Finnish president agreed in Bodø to establish a military transport corridor through northern Norway, Sweden and Finland.[21] In November 2024, the Nordic defence ministers signed a Letter of Intent on strategic corridors for military transport across the wider region.[22] And in May 2025, Nordic transport ministers issued a joint statement explicitly linking military mobility, civil preparedness and security of supply in national transport planning.[23] The overlap became operational in Cold Response 26 in March 2026, when large-scale movement of forces from Sweden into northern Finland formed part of establishing NATO's Forward Land Forces presence there, for which Sweden is the framework nation, with civilian transport and logistics networks carrying the region's capacity to receive and sustain Allied forces.[24] Alliance membership also changes the scale of the task. Security of supply must now stretch to more people, as allied reinforcements and transiting forces arrive; to more places, as Sweden supports Finland and the Baltic states; and over a longer time, for a protracted rather than a short conflict.[25]

21 Government of Norway (2024, 20 June), "Military transport corridor to be established in the north."
22 Government Offices of Sweden, Swedish Treaty Series (2024). "Letter of Intent on military mobility between Nordic countries", signed 21 November 2024, published 22 November 2024.
23 Finnish Government, Ministry of Transport and Communications (2025, 13 May), "Nordic transport ministers issue a statement on military mobility and security of supply."
24 Finnish Ministry of Defence (2026, 16 March), "Joint statement on Cold Response 26 and NATO's Forward Land Forces in Finland by the Ministers of Defence of Finland, Sweden and Norway."
25 Malmberg, P. (2025, 8 June), DN Debatt, *Dagens Nyheter*.

4. From Preparedness to Strategic Resilience

Traditional preparedness – continuity planning, redundancy, emergency stocks, exercises, cyber defence – remains indispensable, but its strategic context has changed. A storm is a straightforward resilience challenge, whereas an adversary probing telecommunications networks or cutting subsea cables to impose costs and constrain political choices is also a strategic challenge. The sequence of shock, response and recovery only addresses part of it. What is required is a transition from resilience as *preparedness for disruption* to resilience as a **strategic capability,** with three dimensions, building on a framework developed in earlier research for the European Parliament on whole-of-society approaches to hybrid threats.[26]

Operational resilience asks whether a system can continue functioning when disrupted: redundancy, backup power, cybersecurity, spare capacity and recovery capability. **Institutional resilience** asks whether the relevant actors can coordinate across organisational boundaries: shared situational awareness, established responsibilities, trusted communication channels. **Strategic resilience** asks a different question: can society preserve its freedom of action while pressure persists and conditions change?

This reframing changes how vulnerability should be analysed. Alongside the traditional question of what threats an operator faces, strategic resilience asks **on whom and on what does our ability to act depends,** moving dependency analysis to the centre of infrastructure policy. Not every dependency is a vulnerability. The objective is therefore not independence but **governable interdependence,** i.e. a condition in which critical dependencies are known, alternatives exist for those that matter most, and the arrangements for switching to them are agreed before they are needed. Dependencies become strategically problematic where they create concentrations that cannot readily be substituted, where control is asymmetric, or where access can be deliberately restricted.

This also changes how redundancy should be understood. Traditional redundancy duplicates critical capacity, but duplication provides false reassurance if the "alternative" system shares the same underlying dependency, as when two telecommunications providers rely on the same cloud platform. The harder question is whether an alternative can actually be switched to, and whether it remains available under the conditions we are preparing for. Not every dependency needs such an alternative, but the ones whose loss would most constrain freedom of action do.

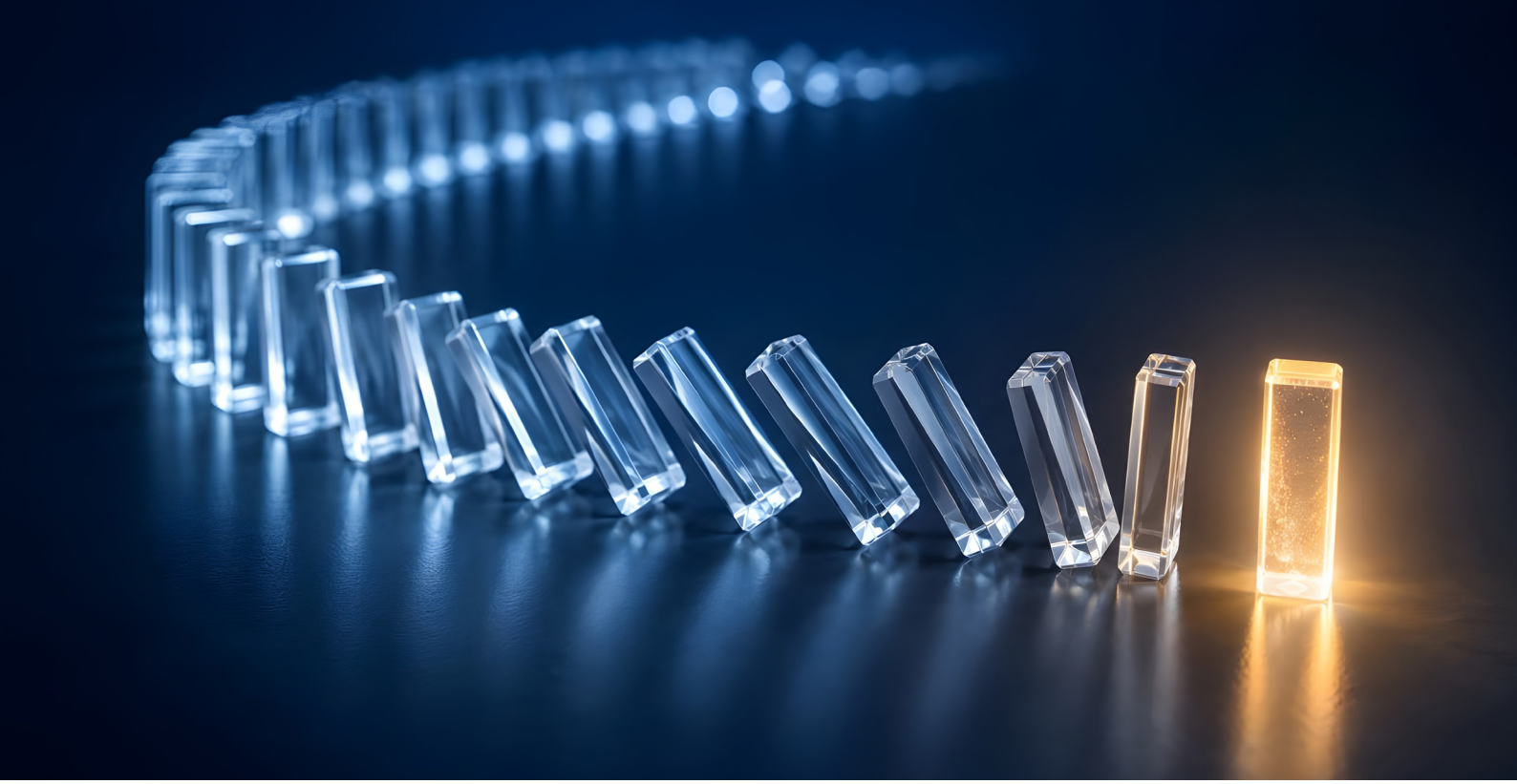
Here public and private incentives diverge. Companies rationally optimise for efficiency and scale in ways that create societal vulnerability, while governments may seek resilience measures whose costs fall on individual operators. Public-private cooperation therefore has to go beyond exchanging information to deciding which options society considers strategically necessary and how their costs are shared. The Niinistö report identifies this gap at EU level, where private-sector expertise is not yet systematically integrated into preparedness policy development and public procurement rules do not yet reflect "preparedness-by-design."[27] Sweden has begun to answer it with preparedness agreements (*försörjningsberedskapsavtal*, "F-contracts") outside the procurement acts: planned in normal times and executed in crisis and war, proportionate, compatible with competition and state-aid rules, resting on Article 346 TFEU. They are now being introduced across 24 agencies, alongside a duty to consider security of supply in procurement.[28] Two further instruments belong in the toolbox. Admitting resilience investment into the regulated asset base of network operators, and a state-backed pool for hostile-state damage that commercial insurers will not cover.

The same logic applies to information and exercises. What is required is **shared situational awareness,** a common enough understanding of threats and dependencies for different actors to make mutually reinforcing decisions, above all in

26 Wigell, M., Mikkola, H. & Juntunen, T. (2021). *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats.* Study for the European Parliament's Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE).

27 Niinistö (2024).

28 SOU 2025:68; Government decision of 18 December 2025 on the 2026 appropriation directives, tasking 24 agencies to identify needs for preparedness agreements.



ambiguous hybrid incidents. Exercises, likewise, should discover capabilities rather than validate plans, with findings feeding into investment and procurement.

Finally, this reframing changes how resilience is valued. Spare capacity, diversified suppliers and alternative connections are often treated purely as costs. This is an error of reference point. Return on investment is measured against normal conditions, which are precisely the conditions resilience is not for. From a strategic-resilience perspective, some of this apparent inefficiency functions as a **strategic option** whose value lies in being available when normal assumptions cease to hold. For the operator, the business case is that the additional cost is offset by what it earns once the force-majeure threshold has been crossed and competitors without the capacity have stopped delivering.

Resilience also bears on deterrence. Hardening and redundancy reduce the damage an attack causes, and with it the chance of holding anyone accountable. The first *Eagle S* ruling found the disruption too minor for criminal charges and Finland without jurisdiction on the high seas, a "resilience dilemma" in which successful protection raises the threshold for consequences.[29] The Court of Appeal's reversal and the *Fitburg* convictions have since established that Finnish courts will hear such cases where the effects are felt in Finland, but the dilemma itself remains. The better the redundancy, the smaller the damage and the weaker the case. Attribution, jurisdiction at sea and enforcement against the shadow fleet therefore have to be designed alongside resilience. The CBSS legal advisers' work and the companion report in this series take that question further.

None of this can be achieved by governments or companies alone. Strategic resilience must be **co-produced,** with both sides jointly identifying dependencies, assessing risk, deciding where additional capability is required and sharing its cost.

29 Ålander & Boulègue (2026).

5. Regionalising Resilience: The Missing Layer

If the first Nordic lesson is that resilience must cross the boundary between government and business, the second is that it must cross national borders. Electricity, telecommunications, subsea cables and the logistics that now support collective defence all run between countries, yet preparedness remains predominantly national.

The Nordic-Baltic region shows this clearly. Small, highly interconnected economies sharing energy systems, maritime spaces and transport corridors, with a more coherent security geography since Finland's and Sweden's NATO accession, but with preparedness arrangements that remain largely national. Strategic resilience therefore requires an intermediate layer, meaning **regional cooperation organised around the geography of critical functions and dependencies,** not around administrative borders. The principle is to organise each resilience function at the level at which the relevant system can actually be governed.

The regional layer has five tasks:

1. **Shared situational awareness,** connecting information held separately by operators, coast guards, regulators and security services so that isolated incidents – a damaged cable, an unusual vessel movement – can be recognised as a pattern.
2. **Cross-border dependency mapping** of a limited number of functions where disruption could cascade across several countries, including shared vendors beneath apparently diversified infrastructure. NESA's *Critical Nordic Flows* study began this work but it has not been carried through.[30]
3. **Regional stress tests** of whether national contingency arrangements survive several countries simultaneously requiring the same alternative capacity, repair resources or transport route.
4. **Recovery as a regional capability,** since no Nordic-Baltic country can rationally maintain every specialised repair capability alone, with subsea cable repair being the clearest example. Converting nominal regional capacity into usable options requires advance agreements or shared inventories.
5. **Joint capability development,** on the model of Baltic Sentry, where cooperation has moved from exchanging information toward jointly developing surveillance and response capabilities.[31]

This does not require a new overarching institution. If anything, the region has too many formats, not always with a clear owner, and the task is to clarify **which existing level performs which function**. National governments remain the foundation of preparedness and operator relationships. Nordic and Nordic-Baltic cooperation connects national systems where infrastructure and dependencies cross borders, with a comparative advantage in political alignment and a manageable group of highly interconnected countries. Its existing instruments are the Haga cooperation between the Nordic ministers responsible for civil preparedness and resilience, renewed by the Haga III declaration of November 2024,[32] sectoral bodies such as NordBER, through which the five Nordic electricity authorities and transmission system operators coordinate contingency planning and exercises,[33] the Nordic Security of Supply Network (NSSN), launched in 2024 on the initiative of Finland's prime minister, with annual meet-

30 National Emergency Supply Agency (2020), *Critical Nordic Flows,* Helsinki.
31 NATO, "Baltic Sentry", and Nordic Energy Research (2026).
32 *Haga III Declaration for the Haga Ministerial Meeting on 27–28 November 2024 in Oslo* (regjeringen.no); Swedish Civil Defence and Resilience Agency, "The Haga cooperation", mcf.se.
33 Danish Energy Agency, "Risk Preparedness", ens.dk/en/supply-and-consumption/risk-preparedness (accessed October 2026): NordBER is the formally established cooperation in which the transmission system operators and energy authorities of the five Nordic countries coordinate contingency planning in the electricity sector.

ings in Copenhagen, Helsinki and Stockholm, and the bilateral NESA–MCF framework described above. The Joint Nordic Declaration on Security of Supply, signed by all five countries together with Åland, the Faroe Islands and Greenland on 2 September 2026, anchors cooperation on public-private security of supply, stockpiling and critical raw materials in the NSSN, launches a joint study, and opens the possibility of a common Nordic security-of-supply agreement to complement or replace the bilateral ones.[34] The Council of the Baltic Sea States (CBSS) can contribute where societal resilience requires broader convening. The Memorandum of Understanding on the protection of critical undersea infrastructure in the Baltic Sea, signed at its Vihula ministerial session on 16 May 2025 by the CBSS member states and the EU, is the broadest such framework in the region, with an expert group through which transmission system operators and infrastructure operators can be drawn in alongside ministries. Its implementation has been central to the CBSS agenda since the May 2026 Sopot ministerial, and Stockholm hosted a meeting of legal advisers on undersea infrastructure on 6 May 2026.[35] The CBSS's role is one of facilitating cooperation rather than operational command. The United Kingdom and the Joint Expeditionary Force add a further layer, as a gap-filler between national and NATO responses and a principal actor on undersea infrastructure. The European Union provides regulatory, economic and financial scale where dependencies or capability requirements exceed regional reach.

These roles inevitably overlap, and the objective should be complementarity. Vulnerabilities should be addressed at the lowest level that has the necessary knowledge and capability, and escalated to the level able to provide additional regulatory, financial or military capacity when required. Coversly, EU and NATO requirements should be translated into operational relationships with the private operators who actually control the infrastructure.

One element remains comparatively underdeveloped, i.e. permanent cross-border mechanisms connecting infrastructure operators with public authorities. This creates a structural mismatch: **companies increasingly operate regionally while preparedness governs them nationally.**

A practical response would be to develop small, function-specific **regional public-private resilience networks**. Each would bring together only the authorities and operators whose decisions determine the resilience of a particular system. Their tasks would be to maintain contact points, review shared dependencies, design stress tests and propose capability investments. This recommendation is not novel. A Nordic public-private resilience network was proposed in 2022 research,[36] has since taken shape as the NSSN, and now has a ministerial declaration behind it. The task is to give it function-specific operational content. Different networks would follow different geographies – Baltic Sea connectivity, Nordic electricity, northern transport and military-mobility corridors. Companies will not commit scarce staff to national, regional and European processes that compete for the same information, so the regional network should be the operator's single point of entry for cross-border functions, with national and EU processes drawing on it rather than duplicating it. This is the most direct way of regionalising the Nordic comprehensive-security logic. It connects the actors responsible for a critical function where the function itself crosses borders.

34 Government Offices of Sweden, Ministry of Defence (2026, 2 September), "Nordisk deklaration om försörjningsberedskap undertecknad", press release.
35 Nordic Energy Research (2026).
36 Wigell et al. (2022), *Nordic Resilience*.

6. Transferring Principles, Not Institutions: Six Tests for Europe

The relevance of the Nordic experience for the rest of Europe depends on distinguishing **institutional models from governance functions**. The relevant question is whether other arrangements can perform the **functions that make Nordic preparedness effective.** The five characteristics of Section 2 therefore return here as five tests of functional equivalence, and Sweden's rebuilding adds a sixth.

Co-production: can public authorities and operators co-produce resilience? Nordic preparedness works well where dense, established relationships already connect regulators and operators. The objective should not be to reproduce Finnish security-of-supply pools specifically, but to ensure some platform or mechanism performs the same function, bringing together the public and private actors whose information and capabilities are required to sustain a critical societal function, whatever institutional form that takes.

Institutionalised trust: can cooperation function without assuming high trust, and can the state require it when it fails? The more useful lesson is that operational trust can be institutionalised. The Swedish conclusion, reached by the Government inquiry and endorsed by the cross-party Defence Commission, is that voluntary cooperation is not sufficient. The law has a gap between peacetime contracts and wartime emergency powers, and a consolidated security-of-supply law including obligations on companies on market terms should be prepared.[37] That sits in open tension with Finland's view that implementing existing EU rules matters more than new regulation, and the tension is worth keeping in view. A model that relies on trust alone is half a model.

Critical societal functions: is resilience organised around functions and dependencies rather than administrative boundaries? Decision-makers should be able to start from a critical societal function and work backwards through the infrastructure, suppliers and capabilities it depends on, choosing the appropriate level – local, national, regional, EU or NATO – for each dependency identified.

Shared capability: do preparedness mechanisms discover and build capabilities, or merely demonstrate compliance? The relevant function is collective learning, requiring an explicit feedback loop from exercise to identified gap to assigned responsibility to capability investment to retest. The obstacle is usually institutional. Exercises become self-contained activities whose findings never reach procurement or regulation.

Permanent preparedness: does the system preserve options under strategic pressure? Nordic countries are small, open economies whose experience does not support an argument for self-sufficiency (Finland, whose security-of-supply system was shaped by historical experience of isolation, is a partial exception). The strategic question is whether that interdependence remains governable when conditions deteriorate, whether credible alternatives exist, or whether apparent alternatives ultimately rely on the same underlying supplier or route. This is the point at which operational resilience becomes strategic resilience.

Mandate and money: are mandates, plans, contracts, resources and follow-up in place, or only cooperation? This sixth test is the one Sweden's rebuilding teaches. Governance and procedures do not by themselves produce capability. The

37 SOU 2025:68; Swedish Defence Commission (2026), *Skärpt läge,* Ds 2026:12.

National Audit Office's finding that steering was too general and funding absent for years is the proof.[38] Three distinct mechanisms serve as criteria: a statutory sector-coordination mandate, a regional node with the authority to act, and a visible, ring-fenced budget line.

The tests also clarify what harmonisation of critical infrastructure protection standards can and cannot achieve. The CER Directive and NIS2 establish a common European floor – identification of critical entities, risk assessments that must consider cross-border dependencies, resilience measures and incident notification – and Finland's own position is that swift and consistent implementation of that floor matters more than new regulation.[39] Harmonisation should therefore be read in two layers. Common legal baselines where cross-border dependencies make divergence dangerous, and functionally equivalent rather than identical arrangements for the cooperation that gives those baselines effect.

The Nordic countries do not themselves pass all six tests. Cross-border dependencies are imperfectly understood, public-private arrangements vary between sectors, regional recovery capabilities are incomplete, and in Sweden capability has lagged behind governance. The Nordic experience therefore offers both **lessons and a laboratory.**



38 Riksrevisionen (2025), RiR 2025:4; Swedish Agency for Defence Analysis (MTFA) (2023); SOU 2025:68, *Nya samverkansformer, modern byggnads- och reparationsberedskap – för ökad försörjningsberedskap.*

39 Government of Finland (2024, November), Ministry of the Interior, "Preparedness Union – Home Affairs", and Ministry of Transport and Communications, "Preparedness Union – Strengthening the EU's Resilience in Transport and Digital Technology".

7. Recommendations: An Agenda for Strategic Resilience

Europe has resilience initiatives in abundance. Its challenge is to connect them across institutional, sectoral and national boundaries. The recommendations below are therefore sorted by who can act on them, and favour a limited set of practical mechanisms over another comprehensive architecture. Sweden is addressed separately because it is the Nordic country rebuilding its system from the ground up.

For the European Union. First, use the Preparedness Union Strategy and the Critical Infrastructure Blueprint to require regional dependency mapping for a small number of critical cross-border functions – electricity and energy connectivity, telecommunications, maritime infrastructure, transport and military-mobility corridors – rather than national asset inventories alone. Second, carry the Cable Security Action Plan through to access. The risk assessment (October 2025), the Submarine Cable Security Toolbox and a €347 million funding call (February 2026) have followed.[40] The next step is to conclude the Baltic Sea agreement on "prioritised availability" of repair vessels that the plan proposes and extend its rules to the planned Cable Vessels Reserve Fleet and to cable spare-part stockpiles, on which the plan is silent about access. Capacity that exists somewhere in Europe is not capacity available to a particular country when several systems fail at once.[41] Third, add strategic-resilience criteria – concentration of dependencies, substitutability, recovery time, defence relevance – to EU co-financing of infrastructure, and recognise preparedness agreements of the Swedish type as a legitimate instrument under the state-aid rules.

For Sweden. Sweden's rebuilt total-defence structures, coordinated on the civil side since 1 January 2026 by the Swedish Civil Defence and Resilience Agency (MCF, the former MSB), give it the means to act on four fronts.[42] First, use the joint study and reporting cycle agreed in the September 2026 Nordic declaration to put the cross-border functions and operator networks identified in this report on the NSSN agenda, and ensure that the common Nordic security-of-supply agreement the declaration envisages covers operator obligations and recovery capacity, not only stocks. Sweden's industrial base is the strategic depth of Finland's, and of the Nordic region's, security of supply, and the agreement should treat it as such. Second, settle the position of privately and foreign-owned operators in total defence – which authority instructs them, how instructions from several governments are reconciled, and how the costs of hostile-state damage are shared – before a sustained campaign forces the question. The Cold War K-company model (*krigsviktiga företag,* firms designated as vital in wartime) is not available. EU procurement, competition and state-aid law rule it out,[43] so the instruments are the F-contracts now being introduced, the consolidated security-of-supply legislation the inquiry proposed, and the Cybersecurity Act, which already gives every NIS2 entity statutory duties to which wartime obligations can be attached. Third, use the Haga III mandate, together with the Nordic Council of Ministers and the Nordic-Baltic Eight (NB8), to give Nordic civil-preparedness cooperation operational content around the cross-border functions identified in this report. Fourth, keep civil and cyber defence connected. The 2026 transfer of MCF's operational cyber functions to the National Defence Radio Establishment separates them just as this report argues for integration, and the operator networks proposed here should span both.

40 European Commission (2026, 11 February), "EU: €347 million to protect Europe's submarine cables", Blue Economy Observatory; Submarine Cable Security Toolbox, February 2026.

41 European Commission and High Representative (2025, 21 February). *Joint Communication on an EU Action Plan on Cable Security,* JOIN(2025) 9 final.

42 Swedish Civil Defence and Resilience Agency (2025, 29 December), "MSB will be Swedish Civil Defence and Resilience Agency as of January 1 2026", mcf.se; Adamson, E. & Ålander, M. (2026, 13 January). "Nordic-Baltic Total Defence: Easier Said Than Done." Heinrich Böll Stiftung.

43 SOU 2019:51, as discussed in SOU 2025:68.

For NATO. Complement the seven baseline requirements for national resilience with civil capability targets for industry and construction and for financial services, as Sweden did when it added preparedness sectors for them. The cost is low and it connects civil resilience to allied defence planning.[44]

For Nordic and Nordic-Baltic formats. Widen and deepen cooperation within the NSSN and extend it, function by function, to the Baltic states. Establish small, function-specific cross-border public-private resilience networks, for which Baltic Sea energy and communications connectivity and the northern transport and military-mobility corridors are natural starting points, tasked with reviewing shared dependencies, designing joint stress tests and proposing capability investment. Turn exercises into genuine regional stress tests, connected to the EU-level stress testing of critical sectors envisaged in the Preparedness Union Strategy, that ask whether national contingency arrangements survive several countries simultaneously requiring the same alternative capacity. Each should end not in a lessons-learned report but in an identified gap, a responsible actor, a corrective action, a deadline and a retest. Treat recovery capacity – subsea repair, specialist components, engineering expertise, construction capacity – as a regional security capability, establishing in advance what exists, who controls it and how access is prioritised, and invest in joint arrangements such as shared stocks and joint procurement and production agreements with industry. Clarify the functional division of labour between existing levels, with no new institutions: national governments as the foundation, Nordic and Nordic-Baltic formats connecting cross-border systems, the CBSS convening more broadly, the UK and JEF filling gaps, the EU providing regulatory and financial scale, and NATO providing capability where resilience meets deterrence.

For infrastructure operators. Map second-tier dependencies (cloud regions, technology vendors, repair providers) and share the decision-relevant parts with the authorities of each jurisdiction in which the company is a critical entity. Treat recovery as a business-continuity and security matter, meaning repair contracts, spares and specialist staff with access terms agreed before demand peaks. And plan now for the sustained-pressure case, defining which government's instructions prevail, how insurance and cost-sharing for hostile-state damage work, and how continuity is maintained under military protection.

These recommendations are best tested together, through a time-limited **Nordic-Baltic Strategic Resilience Pilot** on two functions: Baltic Sea energy and communications connectivity, and the northern transport and military-mobility corridor. Sweden should table it in the NSSN under the 2 September 2026 declaration, with the declaration's joint study as its first phase, Finland and Sweden as framework nations, the Baltic states associated, and financing from national preparedness budgets with EU co-funding where eligible. Two years would allow a dependency assessment, one stress-test cycle and corrective measures. Success should be measured not by meetings held but by capabilities that did not previously exist, i.e. a signed access agreement for repair vessels, a mapped shared-vendor dependency with a mitigation in place, and a corridor stress test with an assigned fix and a retest date. If it delivers, the method can extend to other European infrastructure geographies, with the Nordic-Baltic region serving as a **laboratory for European strategic resilience**.

44 Malmberg, P. (2026, 28 August), Di Debatt, Dagens industri.

Conclusion: From Preparedness to Freedom of Action

The Nordic experience provides Europe with no ready-made blueprint, and Nordic societies are not immune to the vulnerabilities of digitalisation, international supply chains and geopolitical competition. What it demonstrates is a governance principle. Resilience is strongest when produced through permanent relationships between the actors responsible for sustaining critical societal functions, since neither public authorities nor private companies can secure modern infrastructure systems independently. It is strongest, too, when those relationships rest on mandates and money, not goodwill alone. The Nordic achievement was to institutionalise this relationship at national level. The challenge now is to extend it across sectors and borders, where dependencies themselves can become instruments of strategic pressure.

The objective cannot be independence from interdependence, on which European economies depend for prosperity and often for resilience. It must be governable interdependence, meaning the visibility, options, relationships and capabilities needed to keep acting when conditions deteriorate. Nordic comprehensive security and total defence are foundations for this. Their European significance lies in the principle that resilience is a capability built collectively, before it is needed.

Background interviews

Christian Fjäder, Professor of Practice in Societal Resilience, Hanken School of Economics, Finland

Pär Malmberg, Former Chair, Swedish Government's Inquiry on Enhanced Security of Supply, Sweden.

Kari Pelkonen, Senior Specialist, Secretariat of the Security Committee, Finland

Minna Ålander, Analyst at the Stockholm Centre for Eastern European Studies, Swedish Institute of International Affairs, Sweden

Two further interviews were conducted on condition of anonymity

GLOBSEC
IDEAS SHAPING THE WORLD

Vajnorská 100/B
831 04 Bratislava
Slovak Republic

+421 2 3213 7800
info@globsec.org
www.globsec.org