Iceland’s Security and Defence Policy: An Independent Review of the Government’s Strategy

Charlie Edwards

20 November 2025

Key Points

- Iceland’s threat environment has structurally changed. Russia’s unconventional war on Europe, persistent cyber intrusions and strategic economic pressure now intersect with Iceland’s deep reliance on digital connectivity, critical infrastructure and alliances.

- Iceland has the potential to respond at pace, leveraging its high-trust society, strong alliances and digitally capable state. Over the next 12 months, the government should focus on three to five concrete priorities that translate strategic intent into measurable resilience, with the private sector treated as a core security.

- The government has the opportunity to expedite the comprehensive legal review of defence and security legislation, including implementing mandatory foreign-investment screening and clarifying the legal definition and protection of critical infrastructure and operator obligations.

- The government can build on the success of CERT-IS and enhance digital sovereignty and cyber readiness by upgrading the organisation’s capabilities and establishing a 24/7 Security Operations Centre (SOC) to improve threat detection, analysis and response times. The SOC could be structured as a public–private partnership, drawing in critical-infrastructure operators and technology firms to share data, expertise and costs.

- The government should formally establish the Icelandic Futures and Foresight Programme (IFFP) as a strategic mechanism for systematic horizon scanning, scenario planning and forecasting on national-security risks, and to translate these insights into practical resilience measures through public–private information-sharing and joint exercises.

- The government can build on existing work to secure predictable, long-term resource commitments by publishing a baseline of civil-preparedness spending and a multi-year plan towards NATO resilience benchmarks, prioritising the development and retention of specialised human capital.

Contents

Executive summary

Chapter 1: Introduction

Chapter 2: The resilience challenges from hybrid threats

Chapter 3: The 'business' of resilience

Chapter 4: The private sector's role in prevention and anticipation

Chapter 5: Conclusion

Notes

Executive summary

Iceland's new security and defence policy is timely and pragmatic. The policy recognises a structural shift in the threat environment: Russia's unconventional war on Europe, persistent cyber intrusions by state and non-state actors and strategic economic pressure, against the background of Iceland's enduring reliance on alliances and whole-of-society resilience. While public support for NATO has grown over the past few years, support for establishing a national army remains low. The security and defence report therefore focuses on practical resilience, legal modernisation and deeper cooperation with allies and the private sector.

The International Institute for Strategic Studies (IISS) report proposes five priorities for the next 12 months:

1) Protecting critical infrastructure and strengthening societal resilience
2) Building digital sovereignty and cyber readiness by upgrading the Icelandic national Computer Emergency Response Team (CERT-IS) and building a 24/7 Security Operations Centre (SOC)
3) Securing supply chains and economic security and expediting foreign-investment screening legislation
4) Deepening alliance and regional defence cooperation, notably through Nordic Defence Cooperation (NORDEFCO) and host-nation support
5) Implementing governance and legal arrangements, including updating the Defence Act, defining critical infrastructure and operator duties, and clarifying emergency powers.

The government should publish a baseline of current civil-preparedness spending and a three-year plan towards the NATO benchmark for resilience, assigning clear ownership to the National Security Council (NSC) and creating an Implementation Unit with quarterly public reporting. A formal Icelandic Futures and Foresight Programme (IFFP) has the potential to link strategic analysis to investment and exercises, embedding public–private information-sharing and joint training.

Iceland faces national-security risks stemming from traditional and hybrid threats, with a particular focus on the digital domain. The government has an opportunity to turn strategic intent into measurable resilience gains by leveraging its high-trust culture and small-state agility. Present and future threats demand it.

1. Introduction

On 11 March 2025, Minister for Foreign Affairs Þorgerður Katrín Gunnarsdóttir presented a proposal to the Althingi to formulate a policy on Iceland's security and defence.[1] The objectives of the policy were to describe the main security challenges in the short and long term, with an emphasis on external man-made threats; set out Iceland's objectives in international security and defence cooperation; address the necessary defence preparedness and capabilities that must exist in Iceland; and suggest improvements to the legal and institutional framework for defence.

A parliamentary working group was tasked with developing a draft security and defence policy to provide strategic guidance for all stakeholders on government priorities and the overall approach to security policy at a time of rapid international change. The document, *Inntak og áherslur stefnu í varnar- og öryggismálum* (The content and priorities of Iceland's defence and security policy) was drafted by a cross-party group of parliamentarians and national-security experts and published in September 2025.

The policy exercise takes place amidst a gradual recalibration of threat perceptions in Iceland. Historically, Icelandic public-security perceptions have centred overwhelmingly on natural hazards and non-military risks. A large-scale Icelandic survey in late 2016 indicated that the primary threats perceived to state security were overwhelmingly natural hazards (25.8%) and environmental risks/climate change (21%), ranking far above traditional military threats or terrorism.[2] The geopolitical turmoil of recent years has prompted measurable changes in public attitudes towards traditional defence. Support for NATO membership has risen, alongside increased positive sentiment towards US bilateral defence cooperation (60.7%).[3] The public's support for NATO is also reflected in a more recent survey conducted in 2023, which revealed a significant shift in Icelandic public opinion towards greater international alignment and reliance on alliances.[4] Despite increased support for NATO, a recent poll showed a 72% opposition to establishing an Icelandic national military.[5]

According to the report 'Leaning Into Cooperation', this shift towards NATO, the European Union and the United Nations reflects a stronger ideological stance, with Icelanders prioritising protection through multilateral bodies. Perhaps of greater consequence to the government and private sector is that the public's 'pragmatic interest' in economic collaboration with Russia and China has practically evaporated.[6]

Iceland's parliamentarians and policymakers recognise the need to leverage both the public's current concerns on security issues and existing strong understanding of natural hazards in order to successfully frame strategic communications for countering malign threats from states including Russia and China, as well as non-state actors such as organised-crime groups and cyber criminals.

As part of the public consultation, the IISS evaluated the security and defence report and its 13 priorities both with the aim of providing a comparison to similar documents published by

NATO member states[7] and, specifically, to identify how the private sector can play a greater role in national security. The role of Iceland's private sector over past decades has shifted from service provision to active participation in civil protection and preparedness, innovation and strategic coordination. Most NATO member states now treat the private sector as part of national policy and capability, not just as contractors, with companies acting as implementors, project developers, financiers and innovation partners. This is particularly true of the Nordic countries, where a whole-of-society approach implicitly and explicitly identifies the private sector as playing a core role in national security. Iceland's private sector finds itself on the front line, both in terms of those who own and operate critical digital and physical infrastructure and the sector being directly exposed to modern threats like state-sponsored cyber attacks and Russia's hybrid warfare.

This report is divided into four main chapters. Chapter Two looks at the national-security risks to Iceland, including in the digital realm. Cyber-security incidents in Iceland have increased significantly year-on-year,[8] including activity by well-funded, technically capable state-sponsored threat actors focused on espionage within Iceland's network domain.[9] Chapter Three sets out the rationale for private-sector involvement in achieving national-security objectives, and how the government can provide favourable conditions and incentives to encourage companies to participate in and contribute to knowledge development, crisis preparedness and appropriate strategies beyond routine business needs.

Chapter Four sets out the role the private sector plays in anticipating risks and threats. However, achieving effective anticipation through information-sharing faces governance challenges, as operators may be unwilling to share data on vulnerabilities with the government or other operators due to concerns over establishing trust, ensuring the security of shared information, and avoiding competitive disadvantage or legal liability. The concluding section suggests practical ideas and recommendations on how the private sector can be engaged using the 13 priorities as a starting point. The government can move quickly if it narrows the list of priorities and empowers the NSC to own them. Progress should be reviewed regularly. Unlike other Nordic states and allies, Iceland is well placed to leverage its existing social strengths and cultural experiences. The nation's high-trust society and established culture of resilience, regularly refined through its response to natural hazards, offers a foundational mechanism upon which to build national-security consensus and preparedness.

The government should select no more than five priorities over the next 12 months and focus its effort on delivering them. These should include the reform of legal and institutional governance and foreign-investment screening; strengthening critical-infrastructure protection and societal resilience; enhancing digital sovereignty and cyber-security capabilities; and ensuring supply-chain security and economic resilience.

2. The resilience challenges from hybrid threats

Successive governments have framed Iceland's resilience as a whole-of-society task, with uninterrupted critical infrastructure as a core aim.[10] For Iceland, preparedness rests on a whole-of-society approach in which the private sector and civil society help build resilience and keep vital services running. The Icelandic Association for Search and Rescue (ICE-SAR) and the Icelandic Red Cross have formal agreements on civil protection.[11]

As a member of NATO, Iceland has also committed to seven baseline requirements for resilience.[12] These underscore the critical importance of protecting civil infrastructure and essential societal functions in Iceland, reflecting the country's unique challenges as an island state. NATO's focus on critical infrastructure highlights several domains vital to Iceland's strategic and economic existence, particularly civil communications (baseline requirement 6) and transport systems (baseline requirement 7). Iceland serves a crucial function as a logistical hub in the North Atlantic and hosts essential digital infrastructure linking North America and Europe. Consequently, safeguarding civil-communication infrastructure has long been a policy priority for the government, especially the four submarine cables: DANICE, FARICE-1, Greenland Connect and IRIS, on which the country is entirely dependent for uninterrupted data connectivity.[13] The government recognises the vulnerability of the cables and has stated that 'it is impossible to protect the cables from natural disasters or deliberate sabotage. Nor is it feasible to monitor them and ensure their overall security, as they often lie at great depth.'[14]

Furthermore, resilient transport systems are essential for Iceland's economy, which relies on international linkages, and for military mobility, ensuring that NATO forces can move across Alliance territory rapidly in a crisis. Several baseline requirements map directly onto Iceland's non-military vulnerabilities. Resilient energy supplies (baseline requirement 2) must be guaranteed alongside telecommunications and transport. Iceland is largely self-sufficient through renewables, yet generation, transmission and fuel logistics remain exposed. Baseline requirement 4 (resilient food and water resources) includes the risk of supply-chain disruption. Iceland relies on imports of food, fuel, medical supplies and spare parts, so security of supply is a core national concern. The Ministry for Foreign Affairs and the National Police Commissioner, along with other ministries, agencies and companies, are currently in the process of assessing Iceland's resilience against these baseline requirements.[15]

Whilst Iceland's funding for defence has grown by about 20% annually since 2016, significant additional increases will be needed in the coming years to ensure active participation, to fulfil NATO capability targets and to strengthen domestic resilience. At the June 2025 NATO Summit, allies agreed a new benchmark to spend up to 1.5% of GDP on civil preparedness and resilience. For Iceland that equates to approximately 70 billion kronur a year; on current outlays across civil protection, the Icelandic Coast Guard (ICG) and cyber security, Iceland appears below that level, implying a sizeable funding gap to meet the NATO benchmark.

For Iceland, the report on defence and security policy captures national-security risks stemming from traditional and hybrid threats, with a particular focus on the digital domain. This emphasis is consistent with the broader security discourse among Nordic and NATO member states, which stresses that hybrid threats exploit vulnerabilities in open, interconnected societies. As part of this project, the IISS benchmarked the report on defence and security policy with US and European threat assessments.[16] Recent threat assessments by European NATO member states for 2024–25 reveal a complex and escalating security environment defined by state-backed hybrid warfare, persistent cyber threats and the exploitation of democratic vulnerabilities. Russia is consistently identified as the primary and most immediate state threat, with China posing the principal long-term systemic threat, characterised by global ambitions to reshape the rules-based world order. China prefers long-term influence operations in the political, economic and research sectors.[17]

Russia is waging an unconventional war against the West to undermine support for Ukraine. This activity targets critical national infrastructure, logistics and military support routes. Techniques range from reckless navigation near NATO units and GPS jamming, to the use of low-level agents recruited via platforms like Telegram to conduct destructive tasks, often bypassing direct state involvement.[18] Russian state-linked groups focus on persistent access to critical infrastructure and government networks. Meanwhile, social engineering, particularly phishing, is the primary initial intrusion vector for threat actors, accounting for approximately 60% of observed incidents. The top-targeted EU sectors by state-aligned threat groups include public administration, transport, digital infrastructure, energy and health.[19] Ransomware continues to be a dominant concern, often utilising multi-extortion techniques covering the Lock, Encrypt, Delete and Steal actions, thus compromising confidentiality, integrity and availability of assets.[20] Non-physical threats include disinformation and influence operations that erode trust in institutions and deepen social divides. Iceland, like many Nordic countries, is particularly exposed due to its high social-media use and a traditionally high-trust culture.[21]

The government recognises that disinformation campaigns are an important component of hybrid threats. The NSC has established working groups (e.g., on information disorder and COVID-19) to examine the extent of false-information spread and to promote reliable information.[22] To build societal resilience, the government champions awareness campaigns to strengthen critical thinking and media literacy among the public, while actively participating in international forums, including the Nordic-Baltic cooperation group on information disorder, and the Nordic Disinformation Resilience Network.[23] The government will want to consider whether it can go further, with initiatives like Sweden's Psychological Defence Agency, created in 2022 with a mandate to identify, analyse and counter foreign malign information activities, or Finland's National Emergency Supply Agency, which is piloting a new centre of excellence dedicated to countering disinformation operations.

Despite the guarantees provided by NATO and the bilateral agreement with the US, threats like organised crime, terrorism and hostile foreign operations are below the threshold of military conflict. To address these threats and in support of the police, Iceland could build on its existing capabilities and cultural strength, including the success of the search-and-rescue (ICE-SAR) teams, which provide a disciplined, nationwide volunteer force that can deploy quickly in harsh conditions, is trusted by the public and works routinely with police and civil-protection authorities. With modest additional training and a clear mandate, the government could develop specialised teams to support monitoring of critical infrastructure, early warning in remote areas and incident response to hybrid threats that fall below the threshold of armed attack. This requires dedicated funding – which could be partially achieved by moving towards the NATO 1.5% GDP benchmark for civil preparedness – to establish a permanent, domestic security force utilising trained reserves and volunteers (e.g., modelled on the Canadian Rangers).[24] This force could provide reconnaissance, critical-infrastructure protection and host-nation support until allied reinforcements arrived.

3. The 'business' of resilience

There is a strong business case for the private sector to contribute to national security. Stable and open business environments rely on civic freedoms and resilience.[25] A lack of resilience in a business or its supply chain can cause a major disruption to society, impacting its finances and reputation. This mutual interest, protecting the foundations upon which the private sector operates, provides the core reason why the business community needs to be involved in national security. The security and defence report addresses the need to integrate the private sector into Iceland's security framework and offers avenues for engagement and collaboration.[26] It frames the strengthening of societal resilience as the first line of defence for Icelandic society, which mandates collaboration with private actors who manage and operate critical infrastructure.[27]

The rationale for a greater role for the private sector also derives from the inherent vulnerabilities created by the private sector's management and operation of critical infrastructure, as well as its dominance in technological innovation.[28] Businesses are responsible for ensuring the uninterrupted operation of critical infrastructure and strengthening societal resilience to threats of any kind, particularly against natural disasters and man-made hybrid threats.[29]

The cyber domain is a crucial frontier, given that the private sector owns and operates the majority of Nordic critical digital infrastructure.[30] Iceland is regularly and increasingly subjected to cyber threats, incidents and attacks affecting businesses, the media and government agencies.[31] The number of state-sponsored threat actors that are well funded, highly capable and focus on espionage rather than financial gain has increased in Iceland.[32]

Private-sector companies possess the technical expertise, operational knowledge and domain intelligence necessary for national cyber defence, especially given the continual and costly cyber attacks they face. Collaboration through mechanisms like Iceland's CERT-IS exemplifies a public–private partnership focused on building resilience and responding to threats. The effectiveness of national cyber security, including the security of critical data centres and subsea cables, hinges on the cyber-security capabilities of private entities working in partnership with the public sector.

Innovation, research and dual-use technology are primary drivers of national-security capabilities in the twenty-first century. The private sector is the main engine of advancements in data-driven technologies like artificial intelligence (AI), machine learning and advanced microchips. Governments play a critical role in promoting investment, development and innovation in defence and security, focusing on dual-use software and technology for civil and military use. Iceland has opportunities to leverage companies that are strong in energy-related innovation (both geothermal and hydraulic) and cyber security, and should be supported to access international funds like NATO's Defence Innovation Accelerator for the North Atlantic (DIANA), to which Iceland belongs, and Innovation Fund. The 2025 conference on dual-use technologies hosted by Business Iceland with the Ministry for Foreign Affairs and the Federation of Industries, is one example of how the public and private sector work well together.[33]

The private sector also contributes to national-security objectives through logistical support and strategic engagement. Some companies support defence functions by providing services at strategic locations like Keflavík International Airport, which is managed by Isavia. The government could do more to provide companies like Isavia with capabilities such as training, logistics and intelligence support, particularly from former police, intelligence and security personnel working in the private sector.

To achieve this the government should, firstly, encourage a shift in mindset among business leaders so that they recognise their inherent role in national security. This will require the private and public sector forging closer ties through information-sharing and by providing clarity on roles and responsibilities. The latter can be achieved through legislation and regulation to institutionalise accountability. For Iceland, a first step will be to legally define critical infrastructure in order to establish clear obligations and security requirements for private operators who currently operate without them.[34] Adopting investment-screening legislation is also vital to protect sensitive industries and critical infrastructure from undesirable foreign influence, reinforcing national security and resilience. Both initiatives could be part of broader national-security legislation.

Foreign-investment screening has emerged as an area of comprehensive security reform across the Nordic states and wider Europe.[35] Reforms have been driven by the necessity of countering states such as Russia and China, which the US and European governments have identified as utilising strategic investments and research projects to gain access and maximise strategic leverage, specifically targeting key vulnerabilities like 5G systems and critical infrastructure.[36]

Direct and indirect ownership of companies can allow entirely legitimate economic decisions to reduce national resilience.[37] Consequently, governments emphasise foreign-investment screening as a vital measure to protect sensitive industries and critical infrastructure from undesirable foreign influence. The government recognises this urgent need, and adopting investment-screening legislation is considered vital to align with Iceland's allies and to reinforce national security and resilience, necessitating its expedition alongside developing a legal definition of critical infrastructure.

The implementation of investment-screening mechanisms varies between countries, reflecting national-security priorities and best practices that Iceland is encouraged to model. Denmark enacted the Investment Screening Act in 2021 to allow screening and intervention in foreign direct investment (FDI) across critical sectors including defence, information technology (IT) security and infrastructure.[38] Norway likewise screens foreign investment in critical sectors, requiring operators to notify the National Security Authority (NSM) of potential acquisitions.[39] Finland utilises targeted legislation to address national-security concerns related to foreign acquisition of real estate near strategic locations or critical sites, specifically requiring permission for non-EU/EEA entities purchasing such property.[40]

At the European level, the EU Foreign Direct Investment Screening Regulation provides a cooperation mechanism that allows member states to exchange information and raise concerns related to specific FDIs, aiming to counter economic coercion and technology leakage.[41]

Secondly, the government should consider employing incentives and investment tools. Since the private sector will often prioritise financial considerations in security spending, market incentives are often inadequate to motivate investment beyond immediate profitability or mandated requirements.[42] Governments should provide incentives to encourage spending related to business assets and reserve grants for more public areas of protection.[43] Public finance, potentially part of NATO member states' commitment to spend 1.5% of GDP on resilience, should be directed towards helping the private sector to view security spending as an investment rather than just an overhead.

Finally, there are opportunities for collaboration and dialogue to be formalised. Iceland's relatively small size and the high-trust nature of Icelandic society mean the government can build on the existing culture of contingency planning common amongst Icelandic businesses. This culture of preparedness for immediate physical disruptions can be leveraged to build resilience against sophisticated, man-made threats, thus maximising national resilience against both natural hazards and malign threats.

Iceland's nascent national-security community is also in a good position to collaborate. The public and private sectors should identify initiatives that promote platforms for information-sharing among policymakers and owners and operators of critical infrastructure. Work is already under way and can be built on with CERT-IS and similar bodies enhancing threat detection and analysis, encouraging secondments or personnel exchanges between government agencies and private companies, and building cross-sector expertise and trust.

4. The private sector's role in prevention and anticipation

Prevention and anticipation are fundamental to Iceland's national-security model. As an unarmed state reliant on external protection, its primary defence rests on internal resilience and diplomatic management of emerging risks rather than traditional military deterrence. Effective prevention is critical because Iceland is a highly digitalised society with critical infrastructure that is exposed to disruption and external interference, since NATO member states may not be able to provide a timely or effective response to threats like sabotage, terrorism and/or organised crime.

The function of anticipation is formalised by the responsibilities of the NSC, which is mandated to regularly 'assess the situation and the outlook in the field of security and defence' in order to improve capacity for handling future threats.[44] Anticipation also involves strengthening analytical capacity, data collection and intelligence-sharing to enhance situational awareness regarding potential foreign-state threats, cyber attacks, espionage and other hostile activities that often operate covertly under hybrid tactics.[45]

Anticipatory functions that include the timely detection, identification and attribution of threats are crucial, especially given the complex and hybrid nature of modern security challenges. Strengthening cooperation between intelligence, the security services, civil authorities and the private sector is necessary to enhance the ability to detect and identify threats before they escalate into serious disruptions.

The government is aiming to increase its anticipatory functions in several ways, including a push to strengthen CERT-IS through the implementation of an active monitoring and early-warning system capable of tracking real-time indicators of serious threats.[46] The initiative will build on the high levels of trust that exist between government security experts and chief information security officers (CISOs) in the private sector, who will observe threats on their networks from foreign state actors at first hand. The government could go further and establish a 24/7 Security Operations Centre (SOC) capability that is jointly run and managed by the public and private sectors. The SOC capability could also focus on real-time monitoring of critical infrastructure (airports, energy facilities, maritime facilities and subsea cables). Moreover, collaboration should extend to operational readiness, where the private sector can actively participate in government-led exercises and training, a key method for testing and improving societal preparedness.

In 2023, the NSC and the Althingi's Committee for the Future held a joint workshop on projects relating to futures studies and its usefulness in matters concerning national security.[47] The workshop covered futures methodology including trend analysis of societal drivers and methods for developing future scenarios. Building on that foundation, the government could launch an 'Iceland Foresight and Forecasting Partnership' (IFFP) under the Ministry for Foreign Affairs. The IFFP would have a simple aim: to develop common foresight and forecasting methods across the public and private sectors, using a mix of classified and publicly available information to build trust and a common view of the future – both in terms of assessing threats and building resilience. A standing public–private programme could apply a widely used government futures toolkit, supported by an independent foresight institute, and use a proven online forecasting platform. Similar initiatives can be found in the United Kingdom, Finland and Norway.[48]

Establishing the IFFP would address a strategic gap in Iceland's national-security strategy and provide a practical way forward to regularly assess the security environment, with the aim of improving the capacity for handling future threats and enhancing analysis. Furthermore, the concept of a standing public–private programme directly supports the explicit need to build more structured and formalised forums for dialogue between government authorities and private-sector leaders on security and defence issues to bolster resilience and critical-infrastructure protection.

5. Conclusion

The geopolitical turmoil of recent years has prompted measurable changes in public attitudes towards defence. Iceland's politicians and policymakers recognise the need to leverage both the public's current concerns around cyber security and existing strong understanding of natural hazards to successfully frame the government's response to the threat from Russia, China and cyber-crime groups. The consultation report on defence and security policy proposes 13 key priorities, categorised into three areas: international cooperation; domestic defence preparedness, knowledge and capability; and challenges in the legal and institutional environment.

While these priorities are comprehensive, a significant challenge will be the government's ability to implement them. Across Europe and North America, governments are struggling to deliver on their commitments.[49] Budgets are tight, agendas are crowded and public-sector productivity has not recovered evenly since the COVID-19 pandemic. Multi-level governance has created unnecessary friction – be it NATO's commitment to spend 1.5% of GDP on resilience or new EU rules on cyber and critical entities. These multilateral commitments require government ministries and regulators to act in sequence, so, unsurprisingly, timetables slip and accountability blurs. Major programmes compete for the same scarce people and procurement capacity, which pushes implementation to the right and inflates costs.

Iceland shares a number of these challenges, but interviewees were keen to stress the country's advantages. Iceland is relatively small, digitally capable and, in theory, can coordinate decisions quickly. Interviewees suggested that Iceland can still move faster than larger states if it narrows the list of priorities, empowers the NSC to own them, and commits to reviewing progress regularly. And, unlike other larger states, Iceland can leverage its existing social strengths and cultural experiences. The country's high-trust society and established culture of resilience, refined through consistently dealing with natural hazards, offer a foundational mechanism upon which to build national-security consensus and preparedness.

The government should select no more than five priorities over the next 12 months and focus its efforts on delivering them. Based on interviews and research for this report, the government should focus on:

1. Protecting critical infrastructure and strengthening societal resilience
2. Building digital sovereignty and cyber readiness
3. Securing supply chains and economic security (investment screening is one tool within this area)
4. Deepening Alliance and regional security cooperation
5. Implementing the governance and legal arrangements needed to implement the national-security strategy.

The concluding section of this report takes each of these priorities in turn and suggests how the private sector can help deliver them through practical investment, information-sharing and joint exercises.

The first priority is to protect Iceland's critical national infrastructure and strengthen society's overall resilience against all forms of threat and risk. The government can translate strategic intent into measurable action through institutionalised foresight and implementation planning. The IFFP should be formally established to serve as a crucial strategic mechanism, bridging the gap between high-level policy and practical national-resilience implementation. This continuous foresight mechanism, aligning with the NSC's responsibility to regularly assess the security and defence outlook, will improve capacity for handling future threats and enhance strategic analysis. The private sector's role in this area is integral, as businesses, alongside civil society and municipalities, are mobilised as core contributors to national resilience.

The second priority is an opportunity for the government to strengthen and formalise cooperation across the public sector and industry to safeguard critical infrastructure and networks, specifically through enhancing capabilities like CERT-IS. The private sector, particularly banking and telecommunications, experiences cyber attacks, including state-sponsored espionage, on a regular basis and is keen to collaborate with government. Furthermore, more could be made of the private sector's investment, development and innovation in dual-use software and technology, offering cyber-security services and solutions that may be leveraged for national defence and overseas markets.

The third priority concerns secure supply chains and economic security. Currently, the Ministry for Foreign Affairs and the National Police Commissioner, along with other ministries, agencies and the private sector, are in the process of assessing Iceland's resilience against these baseline requirements, given that the security of supply is a core national concern. The protection of Iceland's critical infrastructure and sensitive industry sectors against malign foreign influence should be expedited via a foreign-investment screening mechanism. New legislation can be modelled on best practices found in Nordic partners such as Finland and Norway, who utilise such screening to comprehensively address risks related to national security, security of supply and hybrid threats.

The fourth priority relates to Iceland's defence. The government has an opportunity to deepen and develop regional cooperation on security and defence, notably within NORDEFCO. The private sector's role will be indispensable in delivering on these international commitments, especially in the capacity of host-nation support, which utilises civilian and commercial resources (e.g., transport, communications, energy and logistics) to support military operations and deployments.[50]

The fifth priority is to promote the protection and uninterrupted operation of critical infrastructure. The private sector's role in this area will be integral, as businesses, alongside civil society and municipalities, are mobilised as core contributors to national resilience. This will require clarifying the legal definition and protection of critical infrastructure, setting explicit security standards and preparedness obligations for operators, while formally defining the government's intervention powers during national emergencies.

Notes

[1] Alþingi, Þingskjal 251 (215. mál), 'Tillaga til þingsályktunar um stefnu í varnar- og öryggismálum' [Motion for a parliamentary resolution on defence and security policy from the Minister for Foreign Affairs], Foreign Minister Þorgerður Katrín Gunnarsdóttir, https://www.althingi.is/altext/157/s/0251.html.
[2] Silja Bára Ómarsdóttir, 'Sýn Íslendinga á utanríkis- og öryggismál' / 'Icelanders' Perspectives on Security and Foreign Affairs', *Stjórnmál og stjórnsýsla / Icelandic Review of Politics and Administration*, vol. 14, no. 2, 2018, pp. 1–18.
[3] National Security Council of Iceland, 'Report of the National Security Council on the Implementation of the National Security Policy for Iceland 2021–2022', Government Offices of Iceland, October 2023.
[4] Silja Bára Ómarsdóttir, 'Leaning into Cooperation: Changes in Icelanders' Perspectives on International Politics after Russia's Invasion of Ukraine', Institute of International Affairs, University of Iceland, 2023, https://rafhladan.is/bitstream/handle/10802/32286/Leaning_into_Cooperation_Final.pdf?sequence=1.
[5] Gallup Iceland, 'Þjóðarpúls Gallup: Her á Íslandi' [Gallup National Pulse: A military in Iceland], April 2025 (online survey, fieldwork 21 March–1 April 2025), https://www.gallup.is/documents/983/Puls_0425_Her.pdf.
[6] Ómarsdóttir, 'Leaning into Cooperation'.
[7] See, for example, Norwegian Ministry of Foreign Affairs, 'Setting the Course for Norwegian Foreign and Security Policy. Meld. St. 36 (2016–2017), Report to the Storting (White Paper)'; and Swedish Defence Commission Secretariat, 'The Swedish Defence Commission's White Book on Sweden's Security Policy and the Development of the Military Defence 2021–2025' (unofficial English summary), 2019.
[8] Thorlaug Borg Agustsdottir, 'Securing Iceland's Digital Future: A Call for Political Action', *Internet Policy Review*, 23 August 2024, https://policyreview.info/articles/news/securing-icelands-digital-future/1791.
[9] Report of the Cross-Party Parliamentary Working Group, 'Inntak og áherslur stefnu í varnar- og öryggismálum' [The content and priorities of Iceland's defence and security policy], Government Offices of Iceland, 12 September 2025.
[10] Mikael Wigell et al., 'Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness', FIIA Report 70, Finnish Institute of International Affairs, September 2022, https://fiia.fi/en/publication/nordic-resilience.
[11] Alyson J.K. Bailes and Þröstur Freyr Gylfason, 'Societal Security and Iceland', *Stjórnmál og stjórnsýsla / Icelandic Review of Politics and Administration*, vol. 4, no. 1, 2008, pp. 1–40.
[12] NATO, 'Resilience, Civil Preparedness and Article 3', 13 November 2024, https://www.nato.int/cps/en/natohq/topics_132722.htm.
[13] National Security Council of Iceland, 'Report of the National Security Council on the Assessment of the Situation and Outlook in National Security Matters', 2021. https://www.stjornarradid.is/library/02-Rit--skyrslur-og-skrar/Matsskyrsla%28INT%29_07.05.21.pdf.
[14] *Ibid.*
[15] Althingi, Parliamentary Resolution on a National Security Policy for Iceland (as amended at the 153rd Legislative Session, 2022–2023), https://www.surrey.ac.uk/sites/default/files/2024-09/2023_Iceland.pdf.
[16] See, for example, Danish Security and Intelligence Service (PET), 'Assessment of the Espionage Threat Against Denmark, the Faroe Islands and Greenland', 2023, https://pet.dk/en/-/media/mediefiler/pet/dokumenter/analyser-og-vurderinger/vurdering-af-spionagetruslen-mod-danmark/vurdering-af-spionagetruslen-mod-danmark-2023_uk_web.pdf; Swedish Security Service, 'The Security Service 2024/25', 2025, https://www.sapo.se/ovriga-sidor/other-languages/english-engelska/press-room/swedish-security-services-annual-assesments/the-security-service-2024-25/pdf-version.htmlF version - Säkerhetspolisen; Lithuanian State Security Department (VSD) and Defence Intelligence and Security Service (AOTD), 'National Threat Assessment 2025', February 2025, https://www.vsd.lt/en/reports/national-threat-assessment-2025/#; Europol, 'European Union Serious and Organised Crime Threat Assessment 2025: The Changing DNA of Serious and Organised Crime', European Union, 2025, https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime; and US Office of the Director of National Intelligence, 'Annual Threat Assessment of the U.S. Intelligence Community', March 2025, https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2025/4058-2025-annual-threat-assessment.

[17] Björn Bjarnason, 'Nordic Foreign and Security Policy 2020: Climate Change, Hybrid and Cyber Threats and Challenges to the Multilateral, Rules-based World Order: Proposals', 1 July 2020, https://www.bjorn.is/greinar/nordic-foreign-and-security-policy-2020.

[18] Charlie Edwards and Nate Seidenstein, 'The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure', IISS, August 2025, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2025/08/pub25-095-the-scale-of-russian-sabotage-operations.pdf.

[19] European Union Agency for Cybersecurity, 'ENISA Threat Landscape 2025', October 2025, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

[20] *Ibid.*

[21] Government Offices National Security Council Iceland, 'Report of the National Security Council's Working Group on Information Disorder and COVID-19', 2020, https://www.stjornarradid.is/library/03-Verkefni/Almannaoryggi/Thjodaroryggismal/Information_DisorderCOVID-19_202010.pdf; and see, for example, Nikolas Sellheim and Dwayne Ryan Menezes (eds), *Non-state Actors in the Arctic Region* (Cham: Springer, 2022); and Government of Iceland National Security Council, 'Hybrid Threats: Summary Report of the National Security Council Conference on Hybrid Threats Held at the University of Iceland February 2020', 2020, https://www.stjornarradid.is/library/03-Verkefni/Almannaoryggi/Thjodaroryggismal/Hybrid_Threats.pdf.

[22] V.A. Jóhannsdóttir, J.G. Ólafsson and F.Þ. Guðmundsson, 'Iceland: A Small Media System Facing Increasing Challenges', in J. Trappel and T. Tomaz (eds), *The Media for Democracy Monitor 2021: How Leading News Media Survive Digital Transformation* (Göteborg: Nordicom, University of Gothenburg, 2021), vol. 2, pp. 275–314.

[23] Government of Iceland National Security Council, 'Hybrid Threats'.

[24] Government of Canada, 'Canadian Rangers: Tasks and Operations', https://www.canada.ca/en/ombudsman-national-defence-forces/education-information/caf-members/career/canadian-rangers/tasks-operations.html.

[25] Interview with the author.

[26] Much of this work builds on multiple reports, including, Bjarnason, 'Nordic Foreign and Security Policy 2020: Proposals'; and Wigell et al., 'Nordic Resilience'.

[27] Parliamentary Resolution on a National Security Policy for Iceland (as amended at the 153rd Legislative Session, 2022–2023).

[28] For an in-depth survey of vulnerabilities in critical infrastructure, see Bridget R. Kane et al., 'Threats to Critical Infrastructure: A Survey', RRA2397-2, RAND Corporation, 2024, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2300/RRA2397-2/RAND_RRA2397-2.pdf.

[29] For example, while Faxaflóahafnir (the Associated Icelandic Ports) are owned by the local municipals, the terminal operations are leased to Eimskip and Samskip, which run the main container terminals at Sundahöfn.

[30] Bjarnason, 'Nordic Foreign and Security Policy 2020: Proposals'; Greiningardeild ríkislögreglustjóra (GRD), 'Fjölþáttaógnir' [Hybrid threats], Embætti ríkislögreglustjóra, May 2023.

[31] Greiningardeild ríkislögreglustjóra (GRD), 'Fjölþáttaógnir' [Hybrid threats].

[32] Report of the Cross-Party Parliamentary Working Group, 'Inntak og áherslur stefnu í varnar- og öryggismálum'.

[33] *Ibid*.

[34] For example the UK's definition of critical national infrastructure is: 'Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in: a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or b) Significant impact on national security, national defence, or the functioning of the state'. See UK Department for Science, Innovation and Technology (DSIT), 'Policy paper: PSTN: Critical National Infrastructure Charter', 18 November 2024, https://www.gov.uk/government/publications/public-switched-telephone-network-critical-national-infrastructure-charter/pstn-critical-national-infrastructure-charter.

[35] Christian Fjäder and Johan Schalin, 'Building Resilience to Hybrid Threats: Best Practices in the Nordics', Hybrid CoE Working Paper 31, European Centre of Excellence for Countering Hybrid Threats, 27 May 2024, https://www.hybridcoe.fi/wp-content/uploads/2024/05/20240527-Hybrid-CoE-Working-Paper-31-Building-resilience-to-hybrid-threats-WEB.pdf.

[36] Bjarnason, 'Nordic Foreign and Security Policy 2020: Proposals'.

[37] Daniel K. Jonsson, 'Preparing for Greyzone Threats to the Energy Sector', RUSI Occasional Paper, November 2020, https://static.rusi.org/185_jonsson_web_0.pdf.
[38] Denmark, 'Lov nr. 842 af 10. maj 2021 om screening af visse udenlandske direkte investeringer m.v.' [Investment screening act], entered into force 1 July 2021.
[39] Norway, 'Act Relating to National Security (Security Act), LOV-2018-06-01-24', adopted 1 June 2018; in force 1 January 2019.
[40] Finland, 'Laki eräiden kiinteistönhankintojen luvanvaraisuudesta' [Act on transfers of real estate requiring special permission], 470/2019, in force 1 January 2020, https://www.finlex.fi/fi/lainsaadanto/2019/470.
[41] High Representative of the Union for Foreign Affairs and Security Policy, 'Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy"', Brussels, 20 June 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020.
[42] See Peter R. Orszag, 'Homeland Security and the Private Sector: Testimony Before the National Commission on Terrorist Attacks Upon the United States', 19 November 2003, The Brookings Institution, https://www.brookings.edu/wp-content/uploads/2016/06/20031119-1.pdf.
[43] OECD, 'Good Governance for Critical Infrastructure Resilience', OECD Reviews of Risk Management Policies, 2019, https://www.oecd.org/en/publications/good-governance-for-critical-infrastructure-resilience_02f0e5a0-en.html.
[44] National Security Council of Iceland, 'Lög nr. 98/2016 um þjóðaröryggisráð' [National Security Council Act], 20 September 2016, https://www.althingi.is/lagas/nuna/2016098.html.
[45] Parliamentary Resolution on a National Security Policy for Iceland – No. 26/145 (approved 13 April 2016), as amended by No. 7/153 on 28 February 2023.
[46] Report of the Cross-Party Parliamentary Working Group, 'Inntak og áherslur stefnu í varnar- og öryggismálum'.
[47] Parliamentary Committee for the Future of the Althingi, 'Report of the Committee for the Years 2022 and 2023, parliamentary document 1598 – case 154, 154th legislative session', 23 April 2024.
[48] See, for example, Tom Wells and Charlie Rogers, 'Building Our Vision for Government Technology Scanning', 29 July 2021, UK Government Office for Science (GOS) Futures, Foresight and Horizon Scanning programme, https://foresightprojects.blog.gov.uk/2021/07/29/building-our-vision-for-government-technology-scanning/; and Wigell et al., 'Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness'.
[49] OECD, 'Government at a Glance', 2025, https://www.oecd.org/en/publications/government-at-a-glance-2025_0efd0bcd-en.html.

We are grateful to Varða– Platform for Security and Resilience, a Foobar Foundation initiative for supporting this research.

IISS

The International Institute for Strategic Studies – UK
Arundel House | 6 Temple Place | London | WC2R 2PG | UK
t. +44 (0) 20 7379 7676 **e.** iiss@iiss.org www.iiss.org

The International Institute for Strategic Studies – Americas
2121 K Street, NW | Suite 600 | Washington DC 20037 | USA
t. +1 202 659 1490 **e.** iiss-americas@iiss.org

The International Institute for Strategic Studies – Asia
9 Raffles Place | #49-01 Republic Plaza | Singapore 048619
t. +65 6499 0055 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies – Europe
Pariser Platz 6A | 10117 Berlin | Germany
t. +49 30 311 99 300 **e.** iiss-europe@iiss.org

The International Institute for Strategic Studies – Middle East
14th floor, GFH Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain
t. +973 1718 1155 **e.** iiss-middleeast@iiss.org

IISS The International Institute for Strategic Studies www.iiss.org