Viable Critical Infrastructure

Sustainable Governance Indicators 2024

SGI Sustainable Governance Indicators

BertelsmannStiftung

Indicator

Policy Efforts and Commitment to a Resilient Critical Infrastructure

Question

How committed is the government to updating and protecting critical infrastructure?

30 OECD and EU countries are sorted according to their performance on a scale from 10 (best) to 1 (lowest). This scale is tied to four qualitative evaluation levels.

10-9 = The government is clearly committed to updating basic technical infrastructure.

8-6 = The government is largely committed to updating basic technical infrastructure.

5-3 = The government is somewhat committed to updating basic technical infrastructure.

2-1 = The government is not at all committed to updating basic technical infrastructure.

Switzerland

Score 10

Switzerland's infrastructure in the field of public transportation and roads is excellent. Telecommunications function excellently, although there have been some delays in establishing the glass fiber network (Sager/Kaufmann 2022; 2023). The country's infrastructure in the field of electricity is technically excellent, but depends very much on cooperation with the EU. As long as Switzerland and the EU do not arrive at a bilateral agreement on electricity, there remain serious risks. The Association of Swiss Electricity Companies (VSE 2023) notes: "The fact that Switzerland has no agreement with the EU on cooperation in the electricity sector is causing serious system risks that are already having a negative impact on security of supply and triggering additional costs. Switzerland is dependent on electricity imports in winter. As early as 2025, Switzerland's import capability could be severely restricted."

The Federal Council adopted the National Strategy for Critical Infrastructure Protection (CIP) on 16 June 2023, revising the versions of 2012 and 2017. The Federal Office for Civil Protection (FOCP, Bundesamt für Bevölkerungsschutz) summarizes the strategy as follows:

"Switzerland's new national CIP strategy defines the overriding goals and principles of action for all parties involved. The strategy also identifies eight measures to improve the country's resilience with regard to its critical infrastructure. For example, the responsible supervisory and regulatory authorities have been tasked with examining all sectors for any significant risk of major supply disruption, as well as taking measures to mitigate this. A further measure involves compiling an inventory, to be updated periodically, of the main objects and operators in Switzerland. These can include important hubs for communication, the power

supply, food distribution and the provision of medicines.
The implementation of the national CIP strategy is closely monitored by the Federal Council's Energy, Environment and Infrastructure delegation. The Federal Office for Civil Protection (FOCP) is responsible for coordinating the strategy's implementation, which will be carried out in close cooperation with the operators of critical infrastructure, supervisory and regulatory authorities in various sectors, and the cantons. Although the CIP strategy currently applies indefinitely, the FOCP will assess every four years whether an update is required" (FOCP 2023).

Citation:
Association of Swiss Electricity Companies (VSE, Verband Schweizerischer Elektrizitätsunternehmen). 2023. "https://www.strom.ch/de/politik/stromabkommen"

FOCP (Federal Office for Civil Protection, Bundesamt für Bevölkerungsschutz). 2023. "Critical Infrastructure Protection." https://www.babs.admin.ch/en/aufgabenbabs/ski.html

Sager, Fritz, and David Kaufmann. 2022. "Infrastrukturpolitik: Verkehr, Energie und Telekommunikation." In Handbuch der Schweizer Politik, eds. Yannis Papadopoulos, Pascal Sciarini, Adrian Vatter, Silja Häusermann, Patrick Emmenegger, and Flavia Fossati. 7th edition, 757-784.

Sager, Fritz, and David Kaufmann. 2023. "Infrastructure Policy: Transport and Energy." In The Oxford Handbook of Swiss Politics, eds. Patrick Emmenegger, Flavia Fossati, Silja Häusermann, Yannis Papadopoulos, Pascal Sciarini, and Adrian Vatter. Oxford: Oxford University Press, 585–603. https://doi.org/10.1093/oxfordhb/9780192871787.013.30.

Schweizerische Eidgenossenschaft. 2023. Nationale Strategie zum Schutz kritischer Infrastrukturen. Ganzheitlicher Ansatz zur Sicherstellung der Verfügbarkeit von essenziellen Gütern und Dienstleistungen. Bern: Schweizerische Eidgenossenschaft, BBI 2023 1659. Accessed on 2023 12 10 via https://www.babs.admin.ch/en/aufgabenbabs/ski.html

Finland

Score 9

According to the OECD (2019), Finland has been at the forefront of promoting resilience in its critical infrastructure for the past decade. With an ambitious objective to become the safest country in Europe, Finland's strategic framework for risk governance closely aligns with the OECD Recommendation on the Governance of Critical Risks.

Since 2010, the National Risk Assessment has been a crucial component supporting the comprehensive Security Strategy for Society, which places vital functions at its core. This strategy influenced the 2013 Government Decision on Security of Supply Goals. It aims to ensure the continuity of economic activities and the functionality of critical infrastructure during severe disruptions and emergencies. The critical infrastructure services identified include energy, data communication systems, financial services, transport and logistics, water supply, construction and maintenance, and waste management.

Finland's strategic approach designates sectoral ministries as leaders in ensuring the resilience of critical infrastructure and emphasizes collaboration through public-

private partnerships. The Security of Supply strategy aligns national preparedness principles while also outlining clear roles and responsibilities across various government branches, including at the local level.

This comprehensive strategy underscores the significance of partnerships, well-functioning markets and regulations in achieving critical infrastructure resilience. To facilitate the implementation of these policies, the National Emergency Supply Organization (NESO) serves as a pivotal platform for public and private cooperation. NESO brings together industry and government in sector-specific groups to develop a shared understanding of critical infrastructure risks, vulnerabilities and practical preparedness measures.

Placed under the Ministry of Economic Affairs and Employment, the National Emergency Supply Agency (NESA) plays a central role in conducting risk analysis, coordinating information-sharing, promoting public-private cooperation and mainstreaming the security of supply policies in critical sectors. With over a thousand participating companies in the pooling system, NESA is widely recognized by its stakeholders as an effective governance mechanism for critical infrastructure resilience.

Currently, there is a legislative initiative to bolster national security and enhance societal resilience. The project aims to transpose the directive issued by the European Parliament and the European Council on the resilience of critical entities, which came into effect in January 2023, into national law (Ministry of the Interior n.d.). This involves a comprehensive review and development of both critical infrastructure and its regulatory framework based on national requirements. The ongoing conflict with Russia in Ukraine and significant shifts in the security landscape have heightened the urgency in safeguarding critical infrastructure and reinforcing its resilience.

As part of this strategy, the Critical Entities Resilience Directive introduces new obligations for Finland, necessitating the identification and supervision of critical entities. Finland, which has not yet defined its national critical infrastructure legislatively, is now required to do so. The directive spans 11 sectors: energy, transport, banking, financial market infrastructure, health, food, drinking water, wastewater, digital infrastructure, public administration and space.

In response to a government report on changes in the security environment submitted to parliament in spring 2022, a legislative project was initiated to propose legislation designed to strengthen the resilience of critical infrastructure. Ministries have since reviewed existing national legislation and identified areas for improvement in official duties, leading to the need for centralized organization under the government.

The project, established on 7 December 2022, is scheduled to continue until 31 December 2024. A steering group led by the permanent secretary of the Ministry of the Interior has been appointed to oversee the project, drawing on the expertise of

various ministries. The project will encompass multiple agency functions, with a dedicated expert group assessing the current situation and contributing to the development of new legislation and crisis resilience support and supervision models. Experts from key agencies such as the National Emergency Supply Agency, the Finnish Transport and Communications Agency (Traficom), the Energy Authority, and the National Land Survey of Finland will be involved in the project on an ongoing basis.

Citation:
OECD. 2019. Good Governance for Critical Infrastructure Resilience. Paris: OECD Publishing. https://doi.org/10.1787/02f0e5a0-en

Ministry of the Interior. n.d. "Reform of the Regulation of Critical Infrastructure." https://intermin.fi/en/project/critical-infrastructure

Denmark

Score 8

The changed geopolitical situation, including the explosion of Nord stream II just outside Danish territory, has further increased attention to the topic of critical infrastructure in Denmark.

Denmark has a highly digitized public sector and a citizenry that, on average, is very IT literate. Danes interact with all public bureaucracy through a national identification system called MitID. Consequently, Denmark is vulnerable to potential cyberattacks. Furthermore, given the high levels of political and interpersonal trust in Denmark, the state is somewhat vulnerable to cyberattacks due to insufficiently tight security.

In 2021 the Danish government published a comprehensive plan to enhance cybersecurity (Cybersecurity plan 2021). The plan sets standards for security levels in ministries as well as security standards for contracts between state actors and private companies. Additionally, the plan requires all public entities to adhere to a specified set of technical standards. The plan indicated that 46% of the IT infrastructure in the state was inadequately protected (Cybersecurity plan p. 20). Furthermore, the plan showed that more than 65% of IT systems used by the state did not meet the technical minimum standards expected.

The plan proposes 34 measures for implementation. The most important measures are the establishment of a central unit to oversee the implementation of cybersecurity measures and the creation of a body to continuously monitor the development of cybercrime in order to develop counterstrategies. These two functions will be placed in the Danish Agency for Digital Government (Digitaliseringsstyrelsen) and the Danish Security and Intelligence Service (PET), the internal security police. The plan was scheduled to be updated in 2024, following an evaluation of the current status.

The Center for Cyber Security (CFCS) serves as the national IT security authority. The Center advises Danish public authorities and private companies that support

functions vital to society on preventing, countering and protecting against cyberattacks.

Citation:
Cyber security plan:
https://digst.dk/media/27024/digst_ncis_2022-2024_uk.pdf

France

Score 8

There is no comprehensive public plan for the protection and development of the critical infrastructures that are vital within many domains in France. That being said, plans exist within most individual sectors. In the transport sector, for instance, a planning committee (Conseil d'orientation des infrastructures, COI) was created in 2021, which includes political actors as well as experts. It provides the government with medium- and long-term strategic investment advice concerning the transport infrastructure. In 2023, the COI presented an infrastructure development strategy linked to the objective of fighting climate change. Drawing on this blueprint, the government announced an investment plan entailing expenditure of €100 billion by 2040 to develop transport infrastructures and reduce greenhouse gas emissions within the transport sector. Furthermore, alongside the train company SNCF, local authorities and the EU, the government will implement a New Rail Deal in the field of regional train services.

The presence of critical nuclear plants and nuclear weapons systems makes it vitally important to plan and implement protection strategies. Yet, given the degree of state secrecy in these areas, no public communications specifically address these issues. More specific domain protection has been developed for both the public and private sectors. The Agency for the Security of Information Systems (ANSI) monitors and coordinates strategies dealing with digital technologies. It publishes recommendations in this sector (ANSI 2020).

As most of this sector's actions are not published in the public domain, it is very difficult to precisely assess plans. However, issues dealing with national security have often led to strong and effective responses. Whether the issue has been terrorist threats or natural or technological disasters, service continuity has generally been assured. However, public services (especially hospitals) are regularly subject to hacking attacks, indicating that room for significant improvement still exists. However, France is still ranked in the top 10 of countries worldwide in this domain by the Global Cybersecurity Index (2020).

Citation:
Global Cybersecurity Index. 2020. "Measuring Commitment to Cybersecurity." https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E
France announces EUR 100 billion investment in rail. 2024. "Railway pro, 28 February." https://www.railwaypro.com/wp/france-announces-eur-100-billion-investment-in-rail/

Germany

Score 8

The German National Strategy for Critical Infrastructure Protection (CIP Strategy) was developed in 2009 and serves as the central strategic basis for CIP, although it is not legally binding. The strategy focuses on three main goals: prevention, reaction, and sustainability. This means avoiding serious disruptions and failures of important infrastructure services, minimizing potential consequences if avoidance is not possible, and regularly evaluating measures and analyzing national and international disruptions to foster continuous learning (BMI, 2009).

The CIP strategy does not specify concrete measures, goals, or indicators. Instead, it provides a framework for existing and planned activities, guiding a structured approach to protecting critical infrastructure and coordinating tasks between ministries. It does not include sector-specific action plans but has led to the development of various action plans, programs, and laws for the protection of essential technical infrastructure, such as digital, transport, water, and energy sectors, all of which have precautionary and safeguarding laws.

For instance, the Energy Security Act (Energiesicherungsgesetz) regulates the energy sector, the Water Security Act (Wassersicherstellungsgesetz) covers the water sector, and the Traffic Safety Act (Verkehrssicherstellungsgesetz) governs the transport sector. Additionally, the IT Security Act (IT-Sicherheitsgesetz) addresses the protection of digital infrastructure (BBK, 2020).

To date, Germany does not have a comprehensive law specifically for the protection of critical infrastructure. However, based on the current government's coalition agreement, the BMI proposed a draft law in July 2023 to identify critical infrastructures at the federal level and define minimum standards for CIP operators. The aim is to create a framework that encompasses the various critical infrastructure sectors currently regulated individually (BMI, 2023a).

Germany's policy efforts to protect critical infrastructure mainly focus on cybersecurity. Besides the IT Security Act, the BMI published a cybersecurity strategy in 2016, which was updated in 2021. This updated strategy, resulting from the monitoring and evaluation process, formulates multiple guidelines, fields of action, and strategic goals, including the protection of critical infrastructure from cyberattacks. The strategy outlines measures to prevent and protect against such threats and describes three criteria to monitor the progress of these measures. The strategy is evaluated every four years and is updated every four to six years (BMI, 2021). For the protection of railways and maritime infrastructure, the Federal Police use surveillance measures, including cameras, sensors, and task forces (BMI, 2023b).

The BMI, as the ministry tasked with civil protection, coordinates strategies, measures, and activities related to critical infrastructure protection. It is supported by

the Federal Office of Civil Protection and Disaster Assistance, the Federal Office for Information Security, and the Federal Agency for Technical Relief. In October 2022, the BMI introduced a joint critical infrastructure unit (GEKKIS) to provide situational reports and facilitate structured information exchange between departments to address challenges jointly (BMI, 2023b).

To ensure effective policy implementation, the cybersecurity strategy plans to involve critical infrastructure operators in a nationwide information exchange on a voluntary basis. Operators are also required to regularly submit information on IT security measures to the Federal Office for Information Security (BMI, 2021).

In conclusion, while Germany has policies targeting the protection of critical technical infrastructure, an overall strategy with clearly defined measures is still lacking. However, the government is committed to updating and improving the protection of basic technical infrastructure.

Citation:
BMI. 2009. "Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)." https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.pdf?__blob=publicationFile&v=3
BMI. 2021. "Cyber Security Strategy for Germany 2021." https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/cyber-security-strategy-for-germany2021.pdf;jsessionid=73F6C4FB9C3B6FEBB37E3D5EE960D2C4.live892?__blob=publicationFile&v=4
BMI. 2023a. "Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen." https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html
BMI. 2023. "Schutz Kritischer Infrastrukturen." https://www.bmi.bund.de/DE/themen/bevoelkerungsschutz/schutz-kritischer-infrastrukturen/schutz-kritischer-infrastrukturen-node.html

Japan

Score 8

Japan boasts one of the most advanced critical infrastructures in the world with high-quality transportation and telecommunications networks, administration, financial and medical services, as well as an efficient energy sector. Due to its location in a seismically active zone, state institutions have put substantial emphasis on preparing for emergency situations, such as earthquakes.

Different sectors of critical infrastructure are supervised by different state institutions: information and communication services, as well as government and administrative services by the Ministry of Internal Affairs and Communications; financial services by the Financial Services Agency; aviation and airport, railway, and logistic services by the Ministry of Land, Infrastructure, Transport and Tourism; electric power and gas supplies, and card services, as well as chemical and petroleum industries by the Ministry of Economy, Trade and Industry; and medical and water services by the Ministry of Health, Labor and Welfare.

Japan scored highly in the Global Cybersecurity Index 2020. Information security is regulated by the Basic Policy of Critical Information Infrastructure Protection from

2014, which clarifies the responsibilities of various governmental institutions and critical information infrastructure operators. Guidelines in this field are revised every three years. In 2015, the National Center of Incident Readiness and Strategy for Cybersecurity was established. The center formulates the Cybersecurity Strategy, the Cybersecurity Policy for Critical Infrastructure Protection and other important guidelines in this field. However, indicators to measure the outcomes specified in these documents are rather vague.

Response to emergency situations is coordinated by the deputy chief cabinet secretary for crisis management, who deals with crisis situations other than those related to national defense, such as large-scale natural disasters, shipping or airplane accidents, terrorist attacks, and operations to rescue Japanese citizens abroad. This post was established in 1998 in response to the Great Hanshin Earthquake in Kobe and the sarin subway attack in Tokyo in 1995. In addition, the post of assistant chief cabinet secretary for security affairs was created in 2001. Nevertheless, due to sectoral divisions among bureaucrats, interministerial coordination sometimes remains insufficient. For instance, organizational confusion during the Great East Japan Earthquake in March 2011 led to cognitive dissonance among decision-makers and prolonged disaster-relief activities.

Citation:
Information Security Policy Council. 2014. “The Basic Policy of Critical Information Infrastructure Protection (3rd Edition).” https://www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf

International Telecommunication Union. 2021. “Global Cybersecurity Index 2020.” https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

National Center of Incident Readiness and Strategy for Cybersecurity. “About NISC.” https://www.nisc.go.jp/eng/index.html

Lithuania

Score 8

The government is largely committed to updating the country’s technical infrastructure. However, the focus is on protection rather than upgrading, and the commitment varies depending on the sector. Sectors seen as potentially vulnerable to external threats, such as energy infrastructure, have received more political attention and resources, allowing for connections with partners in the EU and NATO. After the initiation of Russia’s large-scale war against Ukraine in 2022, the government adopted additional measures to protect physical critical infrastructure and data. Planning for the development of military and civilian infrastructure necessary to support the expansion of NATO forces, particularly the stationing of the German brigade beginning in 2027, gathered pace in 2023.

There is extensive regulation aimed at protecting objects important for national security and critical information infrastructure. On the strategic level, these issues are governed by the National Security Strategy, the latest version of which was adopted

in 2021. There are also sectoral strategies, such as the National Energy Strategy. On the operational level, different sectors are regulated by sectoral legislation. For instance, the Law on Cyberswecurity and the government resolution on the objects of critical information infrastructure regulate the protection of these objects from cyberattacks.

Different ministries are responsible for the protection and upgrading of various types of critical infrastructure. The Ministry of Energy is responsible for energy infrastructure; the Ministry of Communications and Transport is in charge of protecting and upgrading transport and other relevant infrastructure; and the Ministry of Defense oversees cybersecurity and military infrastructure development. These policies are coordinated by the government, including during the drafting of yearly budgets.

Cybersecurity and ICT infrastructure have received positive assessments from international organizations. For instance, in the latest Global Cybersecurity ranking (2020), Lithuania was ranked sixth. The upgrading and development of ICT infrastructure, including high-speed internet networks, have benefited from foreign investors and strong competition among service providers, predominantly Nordic companies. However, the upgrading of transport infrastructure such as railways – the Rail Baltica project – and roads has been complicated by delays, often due to lengthy public procurement processes. EU funding provides a significant share of the funds used for upgrading infrastructure.

Citation:
The resolution of the Lithuanian parliament on the adoption of the National security strategy. 2021. No. XIV-795. https://www.e-tar.lt/portal/en/legalAct/f54863b0623a11eca9ac839120d251c4
Vilpišauskas, R. 2021. “Lithuania: Regulatory Patchwork That Evolved in Response to External Threats, Legal Approximation and Domestic Influences.” In Andžans, M., Spruds, A., Sverdrup, U., eds., Critical Infrastructure in the Baltic States and Norway: Strategies and Practices of Protection and Communication. Riga: Latvian Institute of International Affairs, 59-97. https://www.liia.lv/en/publications/critical-infrastructure-in-the-baltic-states-and-norway-strategies-and-practices-of-protection-and-communication-944?get_file=1
The Government Annual Report for 2022, 17 May 2023 (in Lithuanian), https://epilietis.lrv.lt/lt/naujienos/seimui-teikiama-vyriausybes-2022-metu-veiklos-ataskaita
Global Cyber Security Index, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Spain

Score 8

The National Critical Infrastructure Protection Plan (PNPIC), approved in 2016, contains criteria and guidelines for mobilizing operational responses and measures to ensure the constant modification and up-to-date protection of critical infrastructures. The National Security Strategy adopted in 2021 includes the protection of critical infrastructure as a key to addressing threats to Spain’s interests and values.

The PNPIC has frequently been updated. The Administration’s Strategic Sector Plan in 2021 involves the designation of 80 new critical operators and 137 new critical infrastructures. Specific action plans refer to the financial system, nuclear industry,

energy (divided into oil, gas, and electricity), transport (divided into air, rail, maritime, road, and urban transport), water, chemical industry, space, ICT, food, health, and facilities and research.

During the review period, the Royal Decree Law 7/2022 of March 29 was adopted to ensure the security of fifth-generation electronic communications networks and services. According to the law, the National Security Scheme for 5G networks and services shall be reviewed at least every four years or whenever circumstances so advise, under the responsibility of the Minister of Economy and Digital Transformation. Spain ranks fourth among the world's countries in the Global Cybersecurity Index 2020.

The Center for Critical Infrastructure Protection (CNPIC) is the body within the Ministry of the Interior responsible for coordinating and supervising all activities assigned to the Secretary of State for Security regarding the protection of critical infrastructures in the national territory. The CNPIC maintains the National Critical Infrastructure Protection Plan and determines the level of criticality. The CNPIC manages a network of more than 300 entities and around 1,200 security plans, including 12 ministerial departments and autonomous community administrations, to facilitate horizontal and vertical policy coordination and implementation.

Citation:
Royal Decree Law 7/2022 of 29 March.

United States

Score 8

The U.S. strategy for updating and protecting critical infrastructure is distributed across a combination of legislative and executive branch measures. While there is no single binding document, several key documents provide insight into this strategy and reflect the government's commitment to achieving it.

In 2013 President Barack Obama issued Presidential Policy Directive 21. PPD-21 outlines the federal government's approach to enhancing the security and resilience of critical infrastructure and established a risk management framework to identify and assess risks to critical infrastructure. Relatedly, the National Infrastructure Protection Plan (NIPP) was developed by the Department of Homeland Security. NIPP outlines a risk management framework for identifying, prioritizing, and protecting critical infrastructure sectors.

In March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). CIRCIA requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report covered cybersecurity incidents and ransomware payments to CISA.

As is characteristic of U.S. public policy, including that from the Democrats, U.S. critical infrastructure plans tend to rely heavily on the private sector. PPD-21 encourages collaboration between public and private sectors, acknowledging that much critical infrastructure in the United States is privately owned.

There are sector-specific orders relating to critical infrastructure as well. For example, President Joe Biden issued Executive Order 14028, which focuses on improving America's cybersecurity.

Citation:
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity
https://www.energy.gov/ceser/presidential-policy-directive-21
https://www.congress.gov/bill/117th-congress/house-bill/2471/text
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Austria

Score 7

From a comparative perspective on 30 European countries, Austria's overall infrastructure quality has been assessed as clearly above average (11/30; see World Forum data for 2019 and 2020). According to Eurostat, Austria has the second-highest share of trains in inland passenger transport, second only to Switzerland. However, these figures contrast starkly with the notably low high-speed internet coverage, both overall and in sparsely populated areas, where Austria fares near the bottom among European countries. Since high-speed internet is essential for economic development, it should be much higher on the agenda.

Recent Austrian governments have committed to a strategy and roadmap for updating and protecting critical infrastructure. In 2014, the federal government launched a new master plan designed to protect critical infrastructure, created by the Federal Chancellery and the Interior Ministry (Bundeskanzleramt n.d.). This master plan was developed in cooperation with other relevant portfolios, the states, key interest groups, and major companies. It documented the progress made since 2008 and defined new goals.

The principles on which all parties involved agreed were cooperation, subsidiarity, complementarity, confidentiality, and commensurability of measures. The key goal was to provide reasonable support for strategically important companies in developing a "security architecture," which includes risk management, business continuity management, and security management. The protection aspect involves identifying vulnerabilities in critical infrastructure and improving its robustness, recovery, and restoration capacity to guard against destruction or disruption by natural disasters, criminal activity, and terrorism. In 2016, the state governors decided on a new program designed to improve cooperation between state and federal agencies.

As a case study on critical infrastructure protection against electromagnetic threats suggests, Austria has generally pursued a cooperation-based strategy, relying on the self-assessment of strategic companies and organizations (see Jager et al. 2016). Further, the authors found that Austria's particular cooperative nature has proven beneficial for addressing complex solutions at different levels, with responsible authorities willing to acknowledge the advantages of proactively engaging in dialogue with various actors (operators and owners). Scattered stocktaking exercises in different areas, such as those concerning electricity blackouts, suggested that Austria is "fairly well" prepared to successfully handle potential challenges. However, further efforts in certain areas, such as expanding the fiber optic network, are urgently needed.

Efforts to protect critical infrastructure have been high on the current government's agenda. The most recent step marked the launch of a bill in late 2023 to improve the resilience of civil defense organizations and ambulances.

Comparative assessments across OECD countries (see OECD Reviews of Risk Management Policies, Good Governance for Critical Infrastructure Resilience) suggest that Austria, unlike several European countries, has addressed the ongoing challenges in a reasonably serious way.

Citation:
Bundeskanzleramt. n.d. "Österreichisches Programm zum Schutz kritischer Infrastrukturen (APCIP)." https://www.bundeskanzleramt.gv.at/themen/sicherheitspolitik/schutz-kritischer-infrastrukturen.html

https://www.derstandard.at/story/3000000188348/blackout-handynetz

https://www.derstandard.at/story/2000143922969/fuer-den-blackout-nicht-gewappnet-nachholbedarf-fuer-oesterreich-bei-der

Jager, Bettina, Alexander Preinerstorfer, and Georg Neubauer. 2016. "Awareness of the Vulnerability of Critical Infrastructures to IEMI Threats: Lessons from Austria." In Infrastructure Risk Assessment and Management, eds. G. Schleyer et al., 51-62.

https://www.oecd-ilibrary.org/sites/b1dac86e-en/index.html?itemId=/content/component/b1dac86e-en

Belgium

Score 7

Belgium, a densely populated country, has one of the densest road and rail networks in the world. Despite this, its road coverage continues to expand, making it one of the costliest infrastructures to maintain relative to the country's size. However, due to a high debt-to-GDP ratio, infrastructure investment has been relatively low both historically and compared to neighboring countries, leading to a visible decline in the Belgian government's "net capital stock" (Biatour et al. 2017). Despite this, most of Belgium's infrastructure remains in good condition, close to the EU average.

For a long time, infrastructure maintenance lacked a clear strategy. Reactivity was good, keeping roads and rail at a decent to good quality, depending on the sub-

region. However, decisions were typically backward-looking, with maintenance initiated only when significant damage was evident. This approach resulted in sluggish and somewhat disorganized works and building sites (see federal action plan for a circular economy).

One prominent case was the numerous tunnels in Brussels, mostly built in the late 1950s, which were barely maintained due to budgetary constraints. Some had to be closed in emergencies around 2018-2020 due to falling concrete blocks. This prompted the current government of Brussels to initiate a more proactive investment plan.

A similar turnaround is taking place across all regions and at the federal level. Significant adverse events, including climatic catastrophes, massive floods, and infrastructure damage, have driven improvements, aided by the EU's Recovery strategy, which conditions funding on well-developed strategic plans.

Infrastructure management has largely been decentralized, with the federal government and regional governments each having authority over their areas of responsibility. This decentralization led to a relative decline in infrastructure quality in Wallonia (mainly in road and rail) and Brussels (mainly road, although public transport improved), and a relative improvement in Flanders (better roads and large investments in other infrastructure, including digital). Both Flanders and Wallonia developed "2019-2024 plans" containing several multi-year infrastructure renovation measures. Flanders, for instance, has improved the highway networks around its main cities and Brussels (one of the many anomalies of Belgian federalism is that the "Brussels ring" is in Flemish territory, together with Brussels' main airport).

As detailed elsewhere in this report, another crucial turnaround during this legislature concerns electricity production. Previous governments decided to shut down nuclear plants and compensate for the loss in electricity production capacity with green energy, mainly wind farms in the North Sea and photovoltaic production across the country. Russia's war of aggression against Ukraine has revealed the infeasibility of relying on imports, leading the government to delay the closure of some nuclear plants, invest in Small Modular Reactors, and accelerate the deployment of wind and solar energy.

Other crucial infrastructures have been delegated to corporations, some state-owned (e.g., railways or water supply and management), and some largely privately owned (e.g., telecommunication). This allows the government to outsource maintenance costs and professionalize decision-making. The outcome is good for water (though costly) but poor for railways, which suffer from a lack of funding and flexibility to fulfill their targets.

Citation:
Biatour, Bernadette, Chantal Kegels, Jan van der Linden, and Dirk Verwerft. 2017. "Public Investment in Belgium – Current State and Economic Impact." Federal Planning Bureau Working Paper 01-17.

https://www.plan.be/uploaded/documents/201701270618330.WP_1701_11411.pdf
Public Investment in Belgium – Current State and Economic Impact [Working Paper 01-17 - 26/01/2017]
https://www.lesoir.be/544135/article/2023-10-18/les-grands-travaux-se-portent-bien
https://www.lecho.be/opinions/general/le-plan-de-relance-perpetue-les-erreurs-du-plan-marshall/10499038.html
https://www.lesoir.be/538672/article/2023-09-21/plan-de-relance-les-chantiers-nattendent-pas-largent-de-leurope-se-fait-attendre
https://www.consilium.europa.eu/en/press/press-releases/2023/12/08/recovery-fund-council-greenlights-amended-national-plans-for-13-member-states/
http://mobilite.wallonie.be/news/plan-infrastructures-2019-2024
Belgium – Set your infrastructure policies in the right direction https://infracompass.gihub.org/ind_country_profile/bel/
Benchmarking Infrastructure Development – World Bank Group | Economy https://bpp.worldbank.org/economy/BEL

Belgian sources on strategy:
https://nextgenbelgium.be/fr/
https://infra4be.com/
Critical infrastructures – Crisiscenter: https://crisiscenter.be/en/what-do-authorities-do/prevention/critical-infrastructures
Investeren in infrastructuur | Vlaanderen.be: https://www.vlaanderen.be/vlaamse-regering/vlaamse-veerkracht/investeren-in-infrastructuur
Geïntegreerd investeringsprogramma | Vlaanderen.be: https://www.vlaanderen.be/geintegreerd-investeringsprogramma
Infrastructuurprojecten | Vlaanderen.be: https://www.vlaanderen.be/departement-mobiliteit-en-openbare-werken/infrastructuurprojecten
Bovengemeentelijke investeringen – Vlaamse Milieumaatschappij: https://www.vmm.be/water/riolering/timing-en-subsidies/bovengemeentelijke-investeringen
Plan Mobilité et Infrastructures pour tous. 2023. “Plan Mobilité et Infrastructures pour tous.” https://infrastructures.wallonie.be/home/nos-thematiques/voies-de-eau/travaux-et-entretiens/plan-mobilite-et-infrastructures-pour-tous.html
pwi_vd.pdf (wallonie.be) : https://www.wallonie.be/sites/default/files/inline-files/pwi_vd.pdf
Aides aux investissements dans des infrastructures de santé en zone rurale – Portail de l’agriculture wallonne (wallonie.be) : https://agriculture.wallonie.be/aides-aux-investissements-dans-des-infrastructures-de-sante-en-zone-rurale
PIC – PIMACI 2022-24 (wallonie.be) : https://infrastructures.wallonie.be/pouvoirs-locaux/nos-thematiques/infrastructures-locales/batiments-et-voiries/plan-dinvestissement-communal.html
Découvrez nos projets ici | Région de Bruxelles-Capitale (budget.brussels) : https://budget.brussels/fr/showcases/expenses/

Plan d’investissement exceptionnel dans les bâtiments scolaires en FWB – DGI : https://infrastructures.cfwb.be/plan-investissement-exceptionnel/

Construction of infrastructure | BIPT: https://www.bipt.be/operators/construction-of-infrastructure
There is no investment gap in Belgian market, telecom regulator says – EURACTIV.com: https://www.euractiv.com/section/digital/interview/there-is-no-investment-gap-in-belgian-market-telecom-regulator-says/

Canada

Score 7

Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security, or economic well-being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories, and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence.

The governments of Canada, in general, are committed to providing infrastructure and ensuring its protection, from highways and sewers to basic internet availability. Significant infrastructure investments through initiatives like the Investing in Canada Plan prioritize upgrading and securing critical electricity, water, transportation, and telecommunications infrastructure with billions in allocated funding.

Through the Investing in Canada Plan, launched in 2016, the government of Canada committed over $180 billion over 12 years for infrastructure that benefits Canadians – from public transit to trading ports, broadband networks to energy systems, and community services to natural spaces. By 2020 – 2021, the plan had invested over $142 billion in more than 92,000 projects, 95% of which were completed or underway.

Many infrastructure programs began as part of the government's response to the 2007 – 2008 Global Financial Crisis. In 2009, the National Strategy for Critical Infrastructure was launched to strengthen the resiliency of critical infrastructure sectors. The government stated it believed the goal of the National Strategy for Critical Infrastructure was to build a safer, more secure, and more resilient Canada by making improvements among the critical infrastructure sectors. These were listed as:

Energy and utilities
Finance
Food
Transportation
Government
Information and communication technology
Health
Water
Safety
Manufacturing

Key areas of focus include cybersecurity, threat assessment, emergency management, and infrastructure investments. Other actors, like the Canadian Centre for Cyber Security – a part of the Canadian Security Establishment – work on cyber threats to critical systems in sectors like energy, finance, telecommunications, transportation, and government. They share threat intelligence, provide advice and guidance, and have spearheaded new cybersecurity compliance legislation.

Importantly, climate change is creating new challenges for infrastructure policy. As illustrated by the dramatic summer 2023 wildfires, insufficient resources are available to address natural catastrophes related to climate change. To implement more resilient critical infrastructure, further provisions should be made in the context of climate adaptation.

Responsibilities for critical infrastructure in Canada are shared by federal, provincial and territorial governments, local authorities, and critical infrastructure owners and operators – who bear the primary responsibility for protecting their assets and services. The National Strategy supports the principle that critical infrastructure roles and activities should be carried out at all levels of society in Canada.

Citation:
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

https://www.infrastructure.gc.ca/plan/about-invest-apropos-eng.html

Czechia

Score 7

The Czech Republic ranks 28th in the OECD in terms of critical infrastructure, but there is gradual, albeit slow, improvement. Its infrastructure development remains hesitant, with investment heavily dependent on EU support.

The Czech Republic has a dense rail network, with more than 121 km of railways per thousand square kilometers. The major strategic issue for rail transport is decarbonization. The price of EU carbon offset permits has created a strong financial incentive to cut carbon emissions, leading to a plan to electrify half of the remaining 3,000 km by 2030. The rate of development in recent years has been 2.8 km per year, meaning a significant acceleration will be needed to meet the target. There are also plans for high-speed trains, reaching 320 km per hour, for the Prague – Dresden route, with the start planned for 2027.

Water transport has a long tradition in the country but is limited mainly by the total length of navigable river sections. The Vltava and Elbe rivers are used for transporting goods, particularly for long-distance transport of bulk building materials, coal, oil, and its products, as well as containerized goods. However, droughts and low water levels have adversely affected usage in recent years, with the Elbe often too shallow for navigation on many days of the year. There have been proposals to construct more weirs to mitigate this problem, but such projects would be both expensive and effective only if the river is similarly made fully navigable on the German side. The current government is firmly opposed to this.

Additionally, there has long been an idea to link the Danube to the Elbe and the Oder through canals, which would require coordination with Poland, Slovakia, and Austria. The Ministry of Transport investigated this from 2016 – 2018 and judged it to be economically viable. Although a start was approved in October 2020, the project was abandoned by the new government in February 2023. It is worth noting that this idea has been proposed for over a hundred years, with plans developed but never implemented.

The availability of high-speed internet is gradually improving, even in less populated areas. Nevertheless, the share of households with fixed very high capacity network

connections places the Czech Republic in the last third of countries. Coverage is even slightly worse in less populated areas (up to 100 inhabitants per km2). However, as high-speed internet connectivity improves, the risk of cybercrime also increases.

Cybersecurity is managed by the National Cyber and Information Security Agency (Národní úřad pro kybernetickou a informační bezpečnost, NÚKIB), established in 2017 as the central administrative body for cyber security. This includes the protection of classified information in information and communication systems and cryptographic protection. NÚKIB publishes an annual report on the state of cyber security in the Czech Republic.

Citation:
https://nukib.gov.cz/

Estonia

Score 7

Estonia employs several strategies to keep its strategic infrastructure updated and functional. The Transport and Mobility Development Plan 2021 – 2035 (TMDP) covers roads, railroads and water and air transport, with the goal of making the transport system smarter and greener. Based on the TMDP, three sectoral agencies were merged into one institution, the Transport Administration, to increase governance efficiency. To monitor progress, the development plan includes the creation of a transport technology scoreboard, which is not yet in place. The TMDP is divided into sector-specific action plans, one of which is the National Plan of Road Maintenance (THK). Despite the strategic objective of building synergy among different modes of transport, the THK considers only road infrastructure, excluding the railroad network, for example.

The financial plan for road renovation and construction is a crucial part of the THK. It is created based on sectoral needs assessments and the National Budgeting Strategy (RES). RES, a document reflecting a conservative fiscal policy, has led to the underfunding of THK for 2023 – 2026. By some estimates, the funds available to maintain the roads at their current level cover only about half of the necessary expenses (ERR 19.12.2023). Moreover, the failure to complete a four-lane Via Baltica motorway by the 2030 deadline risks incurring a fine from the European Commission (ERR 04.08.2023).

An important area of critical infrastructure is the electricity and telecommunication network. Elering is an electricity and gas transmission system operator responsible for connecting producers, network operators and consumers into a unified system. In addition to physical electricity and gas networks, Elering develops the energy sector’s IT infrastructure, creating opportunities for smart production and consumption solutions. The smart grid enables energy producers and consumers to analyze generated data, increasing efficiency in energy production and consumption.

Elektrilevi is the company responsible for delivering electricity to all customers. The company has a clear investment plan that considers the number of customers connected to power lines and substations, suppliers of essential services, the condition and malfunction risk of power lines, natural conditions, and other infrastructure upgrade plans. In 2023, Elektrilevi's investments totaled €6,651,439 (Elektrilevi 2023). Despite these efforts, rural areas regularly suffer from supply disruptions caused by extreme climate conditions such as snow and storms. The same problems exist with the telecommunications network.

Despite existing strategies that include elaborate governance and coordination mechanisms, as well as benchmarks and monitoring tools, the system has largely remained fragmented and subordinated to the overall goal of fiscal orthodoxy.

Citation:
ERR. 2023. August 8. "Tallinna-Pärnu Maantee Välja Ehitamata Jätmine Võib Tuua Trahvi." https://www.err.ee/1609053344/tallinna-parnu-maantee-valja-ehitamata-jatmine-voib-tuua-trahvi
ERR. 2023. December 19. https://www.err.ee/1609199182/uues-teehoiukavas-on-teede-olukorra-sailitamiseks-pool-rahast

Greece

Score 7

Greece has established a clear strategy and roadmap for updating and protecting critical infrastructure, as outlined in the national reform program (Hellenic Republic 2023) and the "Greece 2.0" Recovery and Resilience Plan agreed upon with the EU (Greek Government 2023). The strategy is binding, reinforced by legislation from the Ministry of Infrastructure and Transport, and adopted by the Greek parliament.

This strategy is detailed in sector-specific action plans, including the "National Action Plan of the Ministry of Infrastructure and Transport" (Ministry of Infrastructure and Transport 2022) and the "Green Transition" and "Digital Transformation" pillars of the "Greece 2.0" plan (Greek Government 2023).

Greece has prioritized enhancing points of entry to increase interconnections and export capabilities, aiming to attract private investment while dedicating public funds to upgrading Aegean Sea ports, national highways, and airports – often through public-private partnerships. However, rail infrastructure has been neglected, as highlighted by a fatal railway accident in February 2023. Railways' share in inland passenger and freight transport remains minimal compared to buses and trucks (Eurostat 2021a and 2021b).

Regarding energy infrastructure, Greece plans to cease lignite plant operations by 2028, shifting toward renewable energy sources and increasing its capacity to import non-Russian natural gas, committing significant infrastructure investments (International Trade Administration 2023).

In digital infrastructure, the government's strategy, outlined in the National Reform and "Greece 2.0" plans, includes an annually updated action plan for digital transformation (Ministry of Digital Transformation 2023). Greece's cybersecurity measures for digital infrastructure are comparable to or exceed those of other EU Member States (International Telecommunication Union 2020: 114).

The Ministry of Infrastructure and Transport leads critical infrastructure projects like roads, ports, airports, and railways, while the Ministry of Digital Governance oversees digital infrastructure. Local executive agencies, such as port authorities, upgrade infrastructure under ministry supervision, and regional projects are managed by regional governments, with central government oversight to ensure effective implementation. Central units regularly monitor, update, and publish policy measures annually (e.g., Ministry of Infrastructure and Transport 2024).

Challenges in implementing these strategies include supply chain shortages, raw material availability, price increases, and limited labor (International Trade Administration 2023).

In summary, while Greece previously ranked poorly among OECD countries for infrastructure quality (World Economic Forum 2019), significant improvements have been made in national roads, ports, airports, and digital infrastructure. Greece has made substantial progress in internet coverage and speed; by mid-2021, 91.7% of Greek households had access to high-speed broadband services (European Commission 2022: 103).

European Commission. 2022. "Broadband Coverage in Europe 2021." https://digital-strategy.ec.europa.eu/en/library/broadband-coverage-europe-2021

Eurostat. 2021a. "Share of buses and trains in inland passenger transport." https://ec.europa.eu/eurostat/databrowser/view/sdg_09_50/default/table?lang=en

Eurostat. 2021. "Share of rail and inland waterways in inland freight transport." https://ec.europa.eu/eurostat/databrowser/view/sdg_09_60/default/table?lang=en

Eurostat. 2021. "High Speed Internet Coverage by Type of Area." https://ec.europa.eu/eurostat/databrowser/view/sdg_17_60/default/table?lang=en

Greek Government. 2023. "Greece 2.0 – Pillars and Components." https://greece20.gov.gr/en/pillars-and-components/

Hellenic Republic. 2023. "National Reform Programme 2023." https://commission.europa.eu/system/files/2023-05/Greece%20NRP%202023.pdf

International Telecommunication Union. 2020. "Global Cybersecurity Index 2020." https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

International Trade Administration. 2023. "Greece – Country Commercial Guide – Infrastructure." https://www.trade.gov/country-commercial-guides/greece-infrastructure

Ministry of Digital Transformation. 2023. "Annual Action Plan 2023." https://mindigital.gr/wp-content/uploads/2023/02/%CE%95%CE%A0%CE%99%CE%A4%CE%95%CE%9B%CE%99%CE%9A%CE%97_%CE%A3%CE%A5%CE%9D%CE%9F%CE%A8%CE%97_%CE%95%CE%A3%CE%94-2023_%CE%A5%CE%A8%CE%94.pdf

Ministry of Infrastructure and Transport. 2022. “National Action Plan 2022.” https://www.government.gov.gr/wp-content/uploads/2021/12/yp_upodomon_2022.pdf

Ministry of Infrastructure and Transport. 2024. “Annual Action Plan 2024.” https://www.ggde.gr/images/attachments/esd_2024_ypyme.pdf

World Economic Forum. 2019. “Global Competitiveness Report.” https://www.weforum.org/publications/global-competitiveness-report-2019/

Ireland

Score 7

Ireland faces capacity challenges in providing infrastructure and services such as housing, healthcare, childcare, transport, energy infrastructure and climate adaptation (NESC 2023; ESRI 2024). Since 2013, the National Risk Assessment has outlined system-wide challenges facing the state, including a critical lack of investment in viable and resilient critical infrastructures. Social partners and think tanks advocate for budget surpluses to be invested in capital projects. Various plans have been stalled due to the lack of critical infrastructure. For instance, planning applications for urgently needed housing cannot proceed in some areas due to the absence of essential infrastructure like water and sewage treatment plants. In other areas, energy supply (electricity) poses a threat to both residential and industrial use patterns.

Fostering national resilience is identified as an important objective in the Strategic Emergency Management: National Structures and Framework (SEM), which focuses on the quick recovery of essential services from emergency events.

The European Council (EC) Directive 2008/114/EC3 requires Member States to identify and designate European Critical Infrastructure (ECI) and assess the need for its protection. This strategy is broken down into sector-specific and sub-sector plans focused on energy, food and water, ICT, finance and financial services, transport, health, public administration, national security, policing, public safety infrastructure and industry. Examples include electric power stations and policing infrastructure. Ireland’s Climate Change Assessment indicates that a sectoral focus on adaptation, without integrative assessment opportunities, increases the risk of underestimating cascading risks – how risks can transfer or flow from one sector to another (Murphy et al. 2023). Approaches to risk screening have been developed to examine vulnerabilities across four critical infrastructure sectors: transport, energy, water and communications. While risk screening is useful for high-level assessment and identifying assets and locations for further analysis, it must be complemented with standardized quantitative approaches for stress testing critical infrastructure, identifying potential failure points, adaptation options and cascading risks.

Citation:
ESRI. 2024. “The National Development Plan in 2023: Priorities and Capacity.” ESRI Survey and Statistical Report Series. https://www.esri.ie/news/irelands-national-development-plan-navigating-substantial-investment-needs-in-housing-health
Murphy et al. 2023. Ireland’s Climate Change Assessment Volume 3: Being Prepared for.
Ireland’s Future Climate https://www.epa.ie/publications/monitoring–assessment/climate-change/ICCA_Volume-3.pdf

Latvia

Score 7

There is a 2021 government regulation on viable critical infrastructure to ensure future business continuity. It serves as a roadmap for updating and protecting critical infrastructure. Based on this regulation, all viable critical infrastructure is divided into three groups, considering several factors: impact on the economy, number of hazards, and general impact on the public. These factors are also crucial for designing business continuity plans.

The Ministry of Internal Affairs is the lead unit in monitoring implementation progress. The ministry reports to the government and European Commission at least once a year. At the municipal level, all municipalities have designed and approved plans for civil protection in case of crises and disasters, according to the Law on Civil Protection and Disaster Management adopted in 2016. The law established the comprehensive civil protection and disaster management framework, including protecting viable critical infrastructure.

Largely due to demographic shifts in Latvia, the use of trains and buses for inland passenger transport is decreasing significantly, from 19.3% in 2015 to 11.3% in 2021, as reflected in Eurostat data. This data also shows that Latvia is improving its high-speed internet coverage, reaching 90.7% in 2021. In the Global Cybersecurity Index (2020), Latvia is ranked 15th with a score of 97.28.

The Rail Baltica connection from Tallinn to Berlin is significant for ensuring quick connections to Western Europe and for increasing the resilience of critical infrastructure. However, due to different track gauges, the rest of the Latvian railway system still needs to be integrated into the Western railway system.

Citation:
Eurostat. Share of buses and trains in inland passenger transport. https://ec.europa.eu/eurostat/databrowser/view/sdg_09_50/default/table?lang=en
2. Eurostat. “High-speed internet coverage by type of area.” https://ec.europa.eu/eurostat/databrowser/view/sdg_17_60/default/table?lang=en
Global Cybersecurity Index 2020. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
Procedures for Surveying Critical Infrastructure, Including European Critical Infrastructure, and Planning and Implementation of Security Measures and Continuity of Operation. 2021. Government Regulation No. 508, 06.07.2021. https://likumi.lv/ta/en/en/id/324689-procedures-for-surveying-critical-infrastructure-including-european-critical-infrastructure-and-for-planning-and-implementation-of-security-measures-and-continuity-of-operation
Civil Protection and Disaster Management Law. https://likumi.lv/ta/en/en/id/282333-civil-protection-and-disaster-management-law
Ministru kabinets. 2020. “Par konceptuālo ziņojumu ‘Par Rail Baltica publiskās lietošanas dzelzceļa infrastruktūras pārvaldību’” https://likumi.lv/ta/id/317018-par-konceptualo-zinojumu-par-irail-balticai-publiskas-lietosanas-dzelzcela-infrastrukturas-parvaldibu

Netherlands

Score 7

Under the oversight of the minister of justice and security, a National Coordinator for Counterterrorism and Security (NCTV) coordinates viable critical infrastructure policies. These cover the areas of energy, telecommunications/internet, transportation, drinking water, surface water, chemicals, nuclear, financial transactions, government information (like civil registration and government-citizen communication), defense – and since very recently. healthcare institutions. This vast policy field is fragmented over seven ministries: Economic Affairs and Climate; Infrastructure and Water Management; Finance; Internal and Kingdom Affairs; Justice and Security; Defense; and Public Health, Welfare and Sports.

In each case, the line ministry establishes general frameworks for the sectors under its responsibility. This includes sectoral policies, laws and regulations, as well as implementation of the "vital cycle" – that is, assessing whether a given process or service is "vital." It also provides support such as simulation and training. The assessment of whether a process or service is vital is made by the responsible line department. This involves analyzing whether the disruption, failure, or manipulation of a process or service could have such serious consequences that it could damage national security.

Within these processes, one or more organizations – such as private companies, independent administrative bodies and parts of the central government – are important for the continuity and resilience of the process. These organizations are referred to as the "vital providers." Vital providers are informed of this status by the line department. Security regions provide support to vital providers in the event of imminent disruption or failure when capabilities are inadequate and public order and safety are at risk. For example, during the COVID-19 pandemic, safety regions were the implementers of lockdown and other public safety measures.

The National Coordinator for Counterterrorism and Security (NCTV) serves as a coordinator in efforts to protect vital infrastructure. This involves a cross-sectoral approach, and entails activities such as drawing up general policy documents and legislation, and developing resilience-enhancing instruments such as the vital cycle. Within the digital domain, the National Cybersecurity Center (NCSC) provides assistance to vital providers, and generates information and advice on threats and incidents.

Although the Netherlands has a reputation for high-quality infrastructure such as roads, waterways and public transport, the Ministry of Infrastructure and Waterways reports a decline: more and longer traffic jams; overdue maintenance for bridges, dikes and river/canal banks; diminishing numbers of bus connections; and more disruptions and less frequent train connections. The ministry has been forced to change its priorities from expansion to maintenance. Another area in which critical

infrastructure is endangered is electricity grid congestion. Several new firms and even citizens trying to install home heating water pumps are lining up, waiting for expansion projects to be completed.

Citation:
Nationaal Coördinator Terrorismebestrijding & Veiligheid (NCTV). "Vitale Infrastructuur, Overzicht Vitale Processen."

NCTV, Rollen en Verantwoordelijkheden

VPNGids.nl. 2023. "Minister Kuipers verklaart zorgsector als vitale infrastructuur." https://VPNGids.nl. Minister Kuipers verklaart zorgsector als vitale infrastructuur

Ministerie van Justitie en Veiligheid, Nationaal Cybersecurity Centrum. 2023. "Cybersecuritybleid Nederland." ncsc.nl

Rijkswaterstaat (Ministerie van I&W). 2023. "Rapport Staat van de Infrastructuur Rijkswaterstaat."

NRC. 2023. "Nederland en Duitsland bundelen hun landmacht. Defensiesamenwerking De bevelhebbers van de Nederlandse en de Duitse landmacht zijn eruit: de gevechtseenheden worden samengevoegd." January 31.

NRC, Benjamin. 2022. "Mobiliteit. NS laat opnieuw minder treinen rijden, en het ov is voor velen nauwelijks meer een manier om op werk of school te komen." NRC October 31.

Portugal

Score 7

The principal strategic document governing the update and protection of critical infrastructure in Portugal is the National Investment Plan 2030 (PNI 2030). Responsibility for critical infrastructure spans various entities within the corporate public sector, which may outsource investments to private firms or engage in public-private partnerships. Notably, Infraestruturas de Portugal (IP) plays a crucial role in overseeing infrastructure quality – including roads, railways, and telecommunications – and has a direct management role, especially in road maintenance. IP oversees the operations of IP Telecom – Serviços de Comunicações SA, a public corporation handling telecommunications infrastructure. Concerning railways, the strategic direction is outlined in the National Railway Plan (Plano Ferroviário Nacional), as stated by the XXII Constitutional Government of the Portuguese Republic (2022). CP – Comboios de Portugal, the public railway company, is primarily responsible for managing rail services and infrastructure. All these public corporations are subject to the joint oversight of the Minister of Finance and the Minister of Infrastructure.

The PNI 2030 emphasizes the need to strengthen territorial cohesion, enhance national infrastructure, and promote sustainable climate action through adaptation to climate change and increased infrastructure resilience. The Recovery and Resilience Plan (PRR) investments in this sector are directed predominantly toward railway and road improvements, as well as advancements in the digital and telecommunications sectors. However, the implementation of the PNI 2030 has fallen well short of what was planned, particularly with regard to rail infrastructure, reflecting prior delays (Cipriano 2023).

In this framework, developing robust telecommunications infrastructure is vital to ensuring secure internet access and enabling daily online activities. According to the Global Cybersecurity Index 2020 (GCI), Portugal has instituted various cybersecurity measures across legal, technical, and collaborative domains. However, there is potential for advancement in organizational strategies and capacity-building. Globally, Portugal ranks 14th on the GCI and holds the eighth position among European nations.

Cipriano, C. 2023. "Governo falha metas PNI 2030 em projetos ferroviários." Público online April 4. https://www.publico.pt/2023/04/04/economia/noticia/governo-falha-metas-pni-2030-projectos-ferroviarios-2044793

International Telecommunication Union (Development Sector). 2020. "Global Index Security 2020." https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

XXII Governo República Portuguesa. n.d. "Plano Nacional de Investimentos 2030 (PNI 2030)." https://www.portugal.gov.pt/pt/gc22/comunicacao/documento?i=apresentacao-do-programa-nacional-de-investimentos-para-2030

XXII Governo República Portuguesa. 2022. "Plano Ferroviário Nacional." https://pfn.gov.pt/wp-content/uploads/2022/11/plano-ferroviario-nacional-20221117.pdf

Governo de Portugal. 2023. "Projetos do PRR das Infraestruturas estão em andamento." https://www.portugal.gov.pt/pt/gc23/comunicacao/noticia?i=projetos-do-prr-das-infraestruturas-estao-em-andamento

Infraestruturas de Portugal. n.d. "2030 Investment Plan (PNI 2030)." https://www.infraestruturasdeportugal.pt/pt-pt/planos-estrategicos

Sweden

Score 7

Preparedness and the protection of critical infrastructure have been at the forefront of governmental discussions for some time, particularly in the two years since Russia invaded Ukraine. This invasion led to the end of the policy of non-alliance and Sweden's NATO membership.

One key aspect of the government's commitment is the development of comprehensive risk management frameworks and collaboration with relevant stakeholders, including private sector entities and international partners. The protection of critical infrastructure in terms of cybersecurity, information security, and communication systems largely falls under the purview of MSB (Myndigheten för samhällsskydd och beredskap). MSB reports on how national policy on critical infrastructure protection aligns with EU policy (Government Offices of Sweden, 2020; MSB n.d.).

Government efforts have focused on cybersecurity, partly due to the high degree of digitalization of services in both the public and private sectors. Other types of critical infrastructure have suffered from chronic underfunding. For instance, the lack of investment in railway infrastructure, combined with increased demand, has brought the system to its knees with delays and frequent cancellations; accidents have also occurred.

Citation:
Government Offices of Sweden. 2020. “EU:s strategi för säkerhetsunionen.”

MSB. (n.d.). https://www.msb.se/en/

Australia

Score 6

For many years until the last decade, there was chronic underinvestment by Australian governments in critical infrastructure. Over the past decade, governments at both federal and state/territory levels have expressed strong commitments to increasing and updating infrastructure in fields such as transport and communication. Despite these efforts, infrastructure remains inadequate due to previous neglect. Additionally, financing these projects remains an ongoing challenge. Typically, the federal government partners with state governments and other stakeholders to fund major infrastructure projects. However, even these joint funding efforts have been insufficient to achieve the ambitious plans set forth by the governments. A recent independent review of over 250 major infrastructure projects nationwide, commissioned by the federal government, recommended that 82 of these projects be scrapped (Grattan 2023). The federal government has indicated it will follow the review’s recommendations. However, state governments, such as the Government of Western Australia, have suggested they may try to find ways to follow through on all their infrastructure commitments (WA Government 2023). A key driver for a comprehensive review has been the cost overruns of several large-scale projects, particularly in major cities like Sydney and Melbourne.

Citation:
Grattan, M. 2023. “Infrastructure Review Recommends Culling 82 Planned Projects.” The Conversation November 16. https://theconversation.com/infrastructure-review-recommends-culling-82-planned-projects-217805

WA Government. 2023. “State Government Affirms Commitment to Projects Following Federal Government Infrastructure Review.” Government of Western Australia. https://www.wa.gov.au/government/media-statements/Cook-Labor-Government/State-Government-affirms-commitment-to-projects-following-Federal-Government-infrastructure-review-20231116

Hungary

Score 6

The National Directorate General for Disaster Management of the Ministry of the Interior oversees disaster management, coordinating activities of other authorities to prevent emergencies. Hungary’s National Security Strategy 2020 addresses several issues concerning foreign liabilities. In this context, an FDI screening mechanism oversees the impact of international companies on national security. Administratively, agencies such as the National Directorate General for Disaster Management and the National Cyber Security Center are responsible for conducting risk assessments and implementing any necessary countermeasures. Especially in the cybersphere, significant developments have occurred. The Recovery and Resilience Plan strongly emphasizes investments in the digital transition, with almost 30% of resources dedicated to such measures. Issues addressed include the availability of

digital equipment in primary, vocational and higher education settings, as well as the digital skills deemed necessary to protect critical infrastructure. Part of the educational effort is focused on raising awareness of problems. The digitalization of the public administration and sectoral improvements in the health, transport and energy sectors are also included.

In the energy sector, progress in decarbonizing energy systems has been notable, especially with regard to the decentralization induced by growing solar energy capacities. This progress reduces dependency on the Paks nuclear energy plant and energy imports from Russia. However, it is projected that even by 2033, the Hungarian energy system will largely rely on nuclear power, with this accounting for an estimated 52% of total energy production (Magyar Nemzet 2023).

Moreover, roads and railroads are in critical condition, with the latter suffering from speed limits on most of its main routes, affecting both passenger transport and cargo (Hungarian Conservative, 2023). A new Ministry of Construction and Transport was established to facilitate and expedite the coordination of infrastructure development projects. However, its operation has led to a number of conflicts between operators and authorities. Nevertheless, parties agreed on a new fare system in late 2023, which lowered ticket prices and improved interoperability (Daily News Hungary 2023).

Citation:
Magyar Nemzet. 2023. “PM Orban: Yes to Green Energy, No to Green Ideology.” 24 November. https://magyarnemzet.hu/english/2023/11/pm-orban-yes-to-green-energy-no-to-green-ideology

Daily news Hungary. 2023. “Complete Overhaul of Hungarian Public Transport Tickets Coming, Extending Free Travel.” 10 December. https://dailynewshungary.com/complete-overhaul-of-hungarian-public-transport-tickets-coming-extending-free-travel/

Hungarian Conservative. 2023. “Men, the State and Rails – How Hungarian Trains are on the Verge of Derailing.” https://www.hungarianconservative.com/articles/opinion/hungarian_railways_obsolete_underfunded_lack-of-vision_eu-funds_internal_conflicts/

Italy

Score 6

Italy’s system for ensuring the viability of critical infrastructure is designed with a multilevel accountability structure. The national coordinator is the president of the Council, supported by the Office of the Military Adviser within the PMO. Additionally, there is the Interministerial Commission for National Defense. Legislation clearly outlines what critical infrastructure operators must do to maintain functionality during critical moments, with specific legal provisions for transport, energy, health, and banking. Each ministry is responsible for monitoring and controlling the implementation of these policies within their respective sectors.

Despite strong and consistent regulations, significant problems persist with the quality of some infrastructure, particularly railways, motorways, and water distribution networks. Cybersecurity has received particular attention, with the

establishment of the national cybersecurity agency in 2021 and the launch of the national cybersecurity strategy for 2022–2026 under the Draghi government.

All governments, especially recent ones, have shown reasonable efforts in ensuring the viability of critical infrastructure. However, by the end of 2023, Italy had not yet adopted the EU directive on critical infrastructure protection (DIRECTIVE (EU) 2022/2557).

Citation:
National Cybersecurity Strategy. 2022. https://www.acn.gov.it/en/strategia/strategia-nazionale-cybersicurezza

New Zealand

Score 6

New Zealand faces significant challenges related to infrastructure deficits in various sectors. The Treasury's 2022 Investment Statement estimates the combined infrastructure gap at $210 billion over the next 30 years under current investment plans. Te Waihanga / New Zealand Infrastructure Commission, established in 2019, estimates that addressing current and future infrastructure requirements would require nearly doubling current spending – from 5.5% of gross domestic product (GDP) to 9.6% over a 30-year period – which would be the equivalent of $31 billion annually to close the gap (RNZ 2022).

Concerns persist that climate change will exacerbate the infrastructure deficit, posing additional challenges to maintaining and upgrading infrastructure. For example, the Treasury calculated that Cyclone Gabrielle and the Auckland Anniversary weekend floods – which struck in early 2023 – caused damages ranging between $9 billion and $14.6 billion (Coughlan 2023). In addition, aging water infrastructure across New Zealand's three waters (i.e., waste, storm and drinking) also requires significant funding and rebuilding. The Labour government launched the Three Waters policy, but it proved highly controversial and became a contentious issue in the lead-up to the 2023 election. At the end of 2023, the new National government announced the repeal of the legislation (Beehive 2023).

There is also apprehension about New Zealand's susceptibility to cyberattacks. In May 2023, the Five Eyes intelligence network issued an alert warning that a group sponsored by the Chinese state had been targeting U.S. critical infrastructure and could direct their efforts to other Western democracies, including New Zealand (RNZ 2023).

In mid-2023, the New Zealand government published a discussion document, acknowledging that the country "is exposed to a wide range of hazards that … can trigger infrastructure failures" as well as recognizing "a range of other threats, such as cyber attacks, espionage and terrorism, which can bring the delivery of crucial services to a halt" (New Zealand Government 2023).

In its 2023 budget, the Labour-Green coalition committed $71 billion for new and existing infrastructure programs, an additional $1 billion for a flood and cyclone recovery package, and $6 billion for a National Resilience Plan. However, critics pointed out that the budget "doesn't make any bold leaps toward infrastructure resiliency" and mainly focuses on "repairing our existing infrastructure" (Shaw et al. 2023).

The government led by Chris Hipkins also introduced the Emergency Management Bill. The bill establishes an amended legal framework that will replace the Civil Defense Emergency Management Act 2002. While the government argued that the bill aims to modernize resilience, critics point out that the new legal framework focuses more on managing the aftermath of disasters and improving civil defense operations rather than on disaster-proofing critical infrastructure (Pennington 2023).

During the 2023 election campaign, the National Party pledged to establish a new National Infrastructure Agency. This agency, tasked with finding private investors and managing the contracting for major infrastructure projects, would also introduce a "value capture" tax on properties benefiting from the completion of significant infrastructure projects (McConnell 2023).

Citation:

Beehive. 2023. "Government to repeal Three Waters Legislation." https://www.beehive.govt.nz/release/government-repeal-three-waters-legislation

Coughlan, T. 2023. "'Hard calls' on cyclone recovery to come – Finance Minister Grant Robertson." New Zealand Herald. https://www.nzherald.co.nz/nz/politics/finance-minister-grant-robertson-to-preach-resilience-in-pre-budget-speech/WEUPSZXFAJGAZECFQXPBZJHIUY

McConnell, G. 2023. "National campaigns for new infrastructure agency, and value capture taxes." Stuff, June 7. https://www.stuff.co.nz/national/politics/300899281/national-campaigns-for-new-infrastructure-agency-and-value-capture-taxes

New Zealand Government. 2023. "Strengthening the Resilience of Aotearoa New Zealand's Critical Infrastructure System." https://consultation.dpmc.govt.nz/national-security-group/critical-infrastucture-phase-1-public-consultation/user_uploads/dpmc–summary-dd–strengthening-the-resilience-of-ci.pdf

Pennington, P. 2023. "Emergency Management Bill flawed, government told by officials." 16 June. https://www.rnz.co.nz/news/political/492100/emergency-management-bill-flawed-government-told-by-officials

RNZ. 2022. "Infrastructure Commission Releases First Long-Term Strategy." 2 May. https://www.rnz.co.nz/news/political/466284/infrastructure-commission-releases-first-long-term-strategy

RNZ. 2023. "NZ Warned After Chinese Hackers Target Critical US Infrastructure – Intelligence Agencies." 25 May. https://www.rnz.co.nz/news/world/490642/nz-warned-after-chinese-hackers-target-critical-us-infrastructure-intelligence-agencies

Shaw, R., et al. 2023. "For a no-frills New Zealand budget it was 'surprisingly frilly': 5 experts on Labour's big pre-election calls." The Conversation, 18 May. https://theconversation.com/for-a-no-frills-new-zealand-budget-it-was-surprisingly-frilly-5-experts-on-labours-big-pre-election-calls-205925

Norway

Score 6

Key infrastructures in Norway include transport (roads, ferries, harbors and rail), energy (hydropower stations with dams, generators and grid), and protection against natural disasters (landslides, avalanches and flooding). In recent years, reliable digital infrastructure and cybersecurity have been added to the list.

Norway has no central ministry or administrative body with national responsibility for maintaining and developing infrastructure, and thus, no overarching national plan for infrastructure modernization. Responsibilities are sectoral, often split among national, regional, and local agencies. This fragmentation, along with a lack of investment and modernization in many areas, has been acknowledged as a challenge.

The Total Preparedness Commission's comprehensive situation analysis from June 2023 proposed a radical change and centralization of all aspects of the security and safety of the population. The title of the report is telling: Now it is serious – Prepared for an insecure future.

To understand Norwegian politics regarding infrastructure investment, two factors are important: The first is the long tradition of Keynesian-inspired economic thinking that public expenditures in infrastructure are key instruments in countercyclical policies. When growth and employment are high and market-driven, public investments should be low and vice versa. The second factor is the tension between the economic interests and needs in urban and rural areas and between national regions. Any ruling government coalition needs the support of center and agrarian parties, whose bases are outside the central regions. The combined effect of these two factors is too low an investment in infrastructure in the central regions, where it is most needed, and often too high investments in remote areas. The low degree of maintenance of critical infrastructure over decades has resulted in a maintenance backlog that will cost substantial sums (estimates from 2021 are at NOK 3.2 trillion) to clear.

Several investment plans exist within different line ministries and sectors, but not all are binding. The most comprehensive and binding plan is the National Transport Plan (NTP). This plan covers a 12-year period and is reviewed by parliament every four years. The overriding objective for the National Transport Plan 2022 – 2033 is an efficient, environmentally friendly, and safe transport system by 2050. A new plan for increased investments in the electricity grid was launched in April 2023. Private businesses have voiced the need for a national plan for digital infrastructure, which the government is currently working on.

In this field, the coordinating agency is the Norwegian Directorate for Civil Protection (DSB). The agency seeks to maintain an overview of vulnerabilities in Norwegian society. Its job is to ensure good preparedness and crisis management

capacity throughout the Norwegian government, and it is the de jure coordinator among ministries in crises. However, its de facto status has not really been tested.

Citation:
Justis – og beredskapsdepartementet. 2023. "Nå er det alvor – Rustet for en usikker fremtid." https://www.regjeringen.no/no/dokumenter/nou-2023-17/id2982767/

Ministry of Transport. 2021. National Transport Plan 2022-2033. White Paper no. 20 (2020-2021) https://www.regjeringen.no/en/dokumenter/national-transport-plan-2022-2033/id2863430/

Rådgivende Ingeniørers Forening. 2021. "Vedlikeholdsetterslep på 3200 milliarder kroner." https://rif.no/vedlikeholdsetterslep-pa-3200-milliarder-kroner/

Energidepartementet og Statsministerens Kontor. 2023. "Regjeringen legger fram handlingsplan for raskere nettutbygging og bedre utnyttelse av nettet." https://www.regjeringen.no/globalassets/departementene/oed/ingrid/regjeringens-handlingsplan-for-raskere-nettutbygging-og-bedre-utnyttelse-av-nettet.pdf

Norwegian Directorate for Civil Protection. n.d. "About DSB." https://www.dsb.no/menyartikler/om-dsb/about-dsb/

Poland

Score 6

Poland has introduced a comprehensive legal framework for managing critical infrastructure. The Law on Crisis Management (2007) and the Law on Anti-Terrorism Activities (2016) are in force. Additionally, the Cybersecurity Strategy for the years 2019 – 2024 was approved by the government on October 22, 2019. The National Infrastructure Protection Plan (Narodowy Program Ochrony Infrastruktury Krytycznej) is updated at least every two years, with the most recent update in 2023.

The plan addresses areas such as energy, communication, telecommunications and information networks, financial systems, food and water supply, wealth protection, transportation, rescue systems, continuity of public administration activities, production systems, and chemical and radioactive substances. These areas fall under a number of different ministries' jurisdictions, but the Government Security Center coordinates these efforts.

Based on information from ministers and voivodes, the director of the Center annually presents an assessment of the program's effectiveness. The Center also serves as the national contact point for institutions of the European Union and the North Atlantic Treaty Organization. An additional supporting body is the Government Plenipotentiary for Strategic Energy Infrastructure, which oversees companies such as Polish Power Grids (Polskie Sieci Elektroenergetyczne), Polish Nuclear Power Plants (Polskie Elektrownie Jądrowe), Gas System (Gaz System) and PERN.

In recent years, the Polish government has undertaken or completed various initiatives connected with the transport system. It introduced the Safe Road Infrastructure program; the Świna Tunnel in Świnoujście opened on June 30, 2023;

the Vistula Spit digging project canal opened on September 17, 2022; and a program intended to build 100 road bypasses was launched. The construction of the Central Communication Port and Via Carpatia is also underway.

On the other hand, Poland's energy infrastructure does not fully meet the country's needs. Electric power lines are old and inefficient and do not support the development and distribution of energy, such as decentralized energy production from renewable sources. This threatens the ability to meet growing demands in the future.

Starting in 2022, the war in Ukraine has been the most significant factor analyzed in terms of critical infrastructure safety. Since February 22, 2022, an elevated and sustained state of emergency has been in effect – the highest in Poland's modern history.

The "strategic" airports, which have gained in importance due to their use in transporting military aid to Ukraine (such as Rzeszów), are the only type of critical infrastructure in Poland subject to systemic control (national and EU) and supervision by state institutions (Biznes Alert 2023). The government has taken steps to enhance security around the LNG terminal in Świnoujście and the Baltic Pipe gas pipeline, which was launched on September 27, 2022.

Poland has also been repelling cyberattacks. Poland was recently ranked in sixth place in the Cyber Defense Index 22/23 (2023), which assesses progress in digitalization and cybersecurity among the world's 20 largest economies. It was acknowledged for implementing a memorandum of understanding, signed with Ukraine in August 2022, to strengthen regional cybersecurity collaboration. However, in terms of AI capacity, Poland's sectoral rank was much lower, at 14th place.

Citation:
Biznes Alert. 2023. "Poland can be a European leader in protecting critical infrastructure if it doesn't shoot itself in the foot." https://biznesalert.com/poland-can-be-a-european-leader-in-protecting-critical-infrastructure-if-it-doesnt-shoot-itself-in-the-foot-interview
MIT Technology Review. 2024. "Cyber Defense Index 22/23." https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23
https://iee.kpi.ua/en/protecting-critical-infrastructure-in-response-to-terrorist-attacks-nato-sps-workshop/

Slovenia

Score 6

Although Slovenia began addressing critical infrastructure protection as early as 2006, comprehensive and systematic regulation was not established until 2017 with the adoption of the Law on Critical Infrastructure. Prior to this, issues related to critical infrastructure were managed through government decisions. The law defines the following sectors as critical infrastructure: energy, transport, food, drinking water supply, health, finance, environmental protection, and information and communication networks and systems. Responsibility for these critical infrastructure

sectors falls to specific ministries related to each sector and the Bank of Slovenia, while management of these infrastructures is more varied. Each sector has a designated contact person, and the Ministry of Defence oversees coordination and provides expert guidance in critical infrastructure.

The National Centre for Crisis Management has been established as an internal unit within the Ministry of Defence. Besides the Law on Critical Infrastructure, other relevant documents include the Resolution on National Security and the Slovenian Defence Strategy. Critical infrastructure protection measures are categorized as ongoing activities; additional activities planned and executed by infrastructure operators or owners; and, if necessary, actions taken by the government to ensure security. According to the risk assessment guidelines 2017 – updated in 2019 – critical infrastructure operators must update their risk assessments if new circumstances arise that could significantly impact infrastructure operations, but at least once annually.

As of 2020, Slovenia ranks 67th globally in the Global Cybersecurity Index. While it has demonstrated strengths in legislative measures, it is comparatively weak in technical measures. The Cybersecurity Strategy was adopted in 2016, and in 2021, the Government Office for Information Security was established as the national authority responsible for information security. Its main task is to enhance resilience against cyber threats that could jeopardize individuals, businesses, the government, and society.

Practice has shown that various state actors and critical infrastructure entities, such as electricity utilities and distribution companies, have been successfully hacked and compromised. These attacks have resulted in the paralysis of government services, theft of personal data, and temporary loss of control over various systems.

Citation:
International Telecommunication Union. 2021. “Global Cybersecurity Index 2020.” https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Dnevnik. 2021. “Hekerji onemogočili portal z zakoni.” Available at https://www.dnevnik.si/1042956169

Monitor. 2023. “Hekerji napadli Holding slovenske elektrarne.” Available at https://www.monitor.si/novica/hekerji-napadli-holding-slovenske-elektrarne/228948/

Ministrstvo za obrambo. 2018. “Predlog programa usposabljanja upravljavcev kritične infrastrukture.” https://dk.mors.si/Dokument.php?id=1307

United Kingdom

Score 6

The National Protective Security Authority (NPSA), an arm of the security services restructured in 2023, is responsible for “building resilience to national security threats,” according to its mission statement. A key focus is on forestalling threats to critical infrastructure, though its mandate extends beyond this. Complementing the NPSA is the National Cyber Security Centre, which provides support for the digital

economy. The UK ranks a close second behind the United States in the Global Cybersecurity Index for the strength of its cyber protections.

Despite the valuable support provided by these agencies, the UK has long faced shortcomings in the quality and capacity of its infrastructure. The protracted development of the HS2 train line northward from London exemplifies these issues, as does the ongoing debate about expanding airport runway capacity in the London area. In October 2023, a decision was announced to halt HS2 construction beyond Birmingham, following a previous decision to cut a planned route connecting to the main east coastline. The prime minister attributed these cuts to escalating costs, described as out of control, but persistent issues with the land use planning system, which empowers NIMBY (not in my backyard) objectors, also inhibit infrastructure development.

To address these challenges, the Infrastructure and Projects Authority was created in 2016. It aims to work with government and industry to deliver projects and improve performance over time. Reporting to the Cabinet Office and the Treasury, it monitors the pipeline of projects and published a strategic plan in 2021 for the decade up to 2030.

Incentives for privatized utilities have also been problematic, particularly in the water industry (in England and Wales), which has faced regular criticism for inadequate investment to prevent sewage spills. Despite issuing fines, the government has struggled to change this pattern.

Israel

Score 5

In 2023, the government passed legislation that includes a list of critical infrastructure projects by categories, including tunnels, electricity, water, oil and gas, transport, and waste. The Ministry of Finance is responsible for coordinating policy regarding critical infrastructure. According to law, critical infrastructure projects will be prioritized over others. Additionally, the relevant government department will appoint a specific individual responsible for coordinating and managing critical infrastructure projects. Furthermore, various regulatory and other barriers that face regular infrastructure projects can be bypassed in the case of critical infrastructure projects. The schedule for critical infrastructure projects will be published publicly.

According to the Planning and Construction Law, the government must establish a ministerial committee for critical infrastructure. The committee is chaired by the prime minister, and its members include the minister of finance, the minister of the interior, the minister of environmental protection and the relevant minister based on the subject matter handled by the committee. A minister who wishes to promote a national planning program related to critical infrastructure must present the program to the ministerial committee and receive its approval before moving forward.

Because this amendment to the law is new, the committee has not yet issued any decisions. The amendment also requires the National Mapping Center to map all infrastructure projects for prioritization. This mapping exercise took place recently; however, no strategic plan has been prepared. The Ministry of Finance is the administrative organization responsible for planning and coordination, but it has not introduced any strategic plan yet.

In 2020, the state comptroller reported that there were many gaps in the readiness of Israel's defense system to protect critical infrastructure from missiles, rockets and other air threats. The comptroller noted that, despite the 2011 decision to safeguard critical infrastructure, no action had been taken. Furthermore, the Ministry of Defense, which is the responsible department in this case, has not provided any operative plans (State Comptroller, 2020).

Citation:
State Comptroller. 2020. "Critical Infrastructure." https://www.mevaker.gov.il/he/Reports/Report_292/0cb33898-55c1-4f7f-a9af-43f5cdc11e9e/part101-izum.docx

Slovakia

Score 5

Law No. 45/2011 Coll. on Critical Infrastructure was enacted on February 8, 2011, to enhance the protection of vital infrastructure, particularly against the escalating threat of terrorist attacks. This legislation aligns with EU Council Directive 2008/114/EC, which pertains to identifying and marking European critical infrastructures and evaluating their protection needs. The new Minister of the Interior plans to draft a new law in this field and establish a new unit dedicated to managing critical infrastructure (Ministry of Interior 2023b).

Critical infrastructure protection encompasses a broad range of issues. Over several years, Slovakia has identified the necessary infrastructure and associated protective tasks. It is essential to understand that safeguarding critical infrastructure is not a one-time effort but a continuous process requiring sustained attention. Departments responsible for individual sectors or operators of critical infrastructure elements must focus continuously on protection, incorporating the latest methods, trends, and knowledge to enhance their practices. Slovakia is a member of the Critical Infrastructure Web Information Network (Ministry of Interior of the Slovak Republic, 2023a).

The National Program for the Protection and Defense of Critical Infrastructure in the Slovak Republic has been established. According to the current law on critical infrastructure and its Annex No. 3, the main sectors and their subsectors under the jurisdiction of central authorities are:

Transport: Managed by the Ministry of Transport and Construction of the Slovak Republic, including subsectors such as road, air, water, and rail transport.

Electronic Communications: Overseen by the Ministry of Transport and Construction of the Slovak Republic, encompassing subsectors such as satellite communications, networks and services of fixed electronic communications, and mobile electronic communications.
Energy: Under the Ministry of Economy of the Slovak Republic, including subsectors like mining, electric power, gas, oil, and oil products.
Post: Managed by the Ministry of Transport and Construction of the Slovak Republic, overseeing postal services, postal payments, and procurement activities.
Industry: Overseen by the Ministry of Economy of the Slovak Republic, including subsectors such as the pharmaceutical, metallurgical, and chemical industries.
Information and Communication Technologies: Under the Office of the Deputy Prime Minister of the Slovak Republic for Investments and Informatization, focusing on information systems and networks.
Water and Atmosphere: Managed by the Ministry of the Environment of the Slovak Republic, including subsectors such as meteorological services, water structures, and the provision of drinking water.
Healthcare: Under the Ministry of Health of the Slovak Republic.
Finance: Managed by the Ministry of Finance of the Slovak Republic, including subsectors such as banking, financial markets, and public finance management systems (Santusová & Jakubík, 2020).
Infrastructure in the Slovak Republic is highly vulnerable and interconnected. The wide range of issues related to its protection reflects the critical importance of infrastructure for society in Slovakia (Santusová & Jakubík, 2020).

Citation:
45/2011 Z. z. Zákon o kritickej infraštruktúre. 2011. Law no. 45/2011 Coll. https://www.zakonypreludi.sk/zz/2011-45

Ministry of Interior of the Slovak Republic. 2023a. “Protection of critical infrastructure.” https://www.minv.sk/?Ochrana_kritickej_infrastruktury_1

The National Program for the Protection and Defense of Critical Infrastructure in the Slovak Republic. https://www.mhsr.sk/uploads/files/c2CSdqQ5.pdf

Ministry of Interior of the SR. 2023. “Press Release.” https://www.minv.sk/?tlacove-spravy-4&sprava=vlada-schvalila-navrh-noveho-komplexneho-ramca-procesov-a-postupov-pre-krizove-riadenie-slovenskej-republiky

Santusová, D., and Jakubík, P. 2020. “Kritická infraštruktúra v Slovenskej republike.” Bezpečnostní teorie a praxe 3/2020. https://veda.polac.cz/wp-content/uploads/2020/11/Kriticka-infrastruktura-v-Slovenskej-republike.pdf

Address | Contact

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Germany
Phone +49 5241 81-0

Dr. Christof Schiller
Phone +49 30 275788-138
christof.schiller@bertelsmann-stiftung.de

Dr. Thorsten Hellmann
Phone +49 5241 81-81236
thorsten.hellmann@bertelsmann-stiftung.de

www.bertelsmann-stiftung.de
www.sgi-network.org

SGI Sustainable Governance Indicators

BertelsmannStiftung