שותפות באנרגיה
ישראל - גרמניה
Energy Partnership
Germany – Israel

Digitalisation and Cyber Security in the Energy Sector

A comparative analysis between Germany and Israel carried out under the bilateral energy partnership on behalf of the German Federal Ministry for Economic Affairs and Energy

Imprint

Published by:
Deutsche Energie-Agentur GmbH (dena)
German Energy Agency
Chausseestrasse 128 a
10115 Berlin, Germany
Phone: +49 30 66 777-0
Fax: +49 30 66 777-699
E-mail: info@dena.de
www.dena.de

Authors:
Dr.-Ing. André Kummerow (Fraunhofer IOSB-AST)
M.Sc. Robin Patrick Williams (Fraunhofer FIT)
M.Sc. Ömer Sen (Fraunhofer FIT)
Mag. Anna Poblocka-Dirakis (dena)

Design & layout:
Heimrich & Hannot GmbH

Last updated:
06/2025

Energy partners:

Federal Ministry for Economic Affairs and Energy
Federal Ministry of the Interior and Community
Ministry of Energy and Infrastructure
www.energy.gov.il
שותפות באנרגיה ישראל - גרמניה
Energy Partnership Germany – Israel

Implementing organisation:

dena

Contents

1 Introduction

1.1 Motivation and goals of study

In the rapidly evolving electrical energy sector, the use of digital technologies is essential to create flexible and decentralised energy systems, enabling an efficient, reliable and sustainable energy supply. The advent of innovative technologies, such as smart metering, cloud and edge computing, blockchain, smart contracts, AI and machine learning, enhances operational efficiency and responsiveness. However, this digital transformation also exposes the sector to significant cybersecurity risks. As part of the energy transition from central fossil power plants to distributed renewable energies, prioritising cybersecurity is essential to protect critical infrastructure and to ensure a safe and resilient energy system.

To meet these challenges, the future strengthening of the energy infrastructures has been an issue of increasing concern for the German and Israeli governments. Launched in 2022, the German-Israeli Energy Partnership (see Section 1.2) formed the framework for this study to enable a productive exchange of knowledge between both countries. This study aims to compare the level of digitalisation and cybersecurity in Germany and Israel and to provide a basis for a strategic prioritisation of future cooperations.

For this, the study pursues the following objectives:

1. Provide a **high-level overview** of the current situations and grand strategies regarding digitalisation and cybersecurity in Germany and Israel.
2. Convey a **detailed understanding of digitalisation** of the German and Israeli energy sector and analyse their transformation towards sustainability and efficiency.
3. Detail the **cybersecurity architecture** in both countries and offer insights into systemic vulnerabilities and **relevant cyber threats** that could harm or destabilise the electrical grid.
4. Analyse **and compare the level of digitalisation and cybersecurity** between Germany and Israel using a comprehensive set of qualitative and quantitative indicators.
5. Provide **recommendations and possible future projects** based on digitalisation and cybersecurity challenges and innovations in both countries.
6. Enhance the **foundation for further cooperation** between Germany and Israel by promoting the importance of cybersecurity in the digitalised energy sector on a global level, which can yield significant benefits for both nations.

The study's research encompasses national developments and trends in digitalisation at different energy infrastructure levels and gives national and international insights regarding cyber threats targeting critical infrastructures and energy systems. This is rounded out by considerations regarding the infrastructure and regulatory frameworks as well as the political conditions in Germany and Israel. The study analyses the state of digitalisation in selected areas of the energy sectors (see Section 1.3) and evaluates systemic vulnerabilities and cyber threats that are particularly relevant for these areas concerning the system's susceptibility and criticality. The comparative analysis of this study follows a systematic approach. This involves the derivation of quantitative and qualitative indicators using generally recognised metrics based on existing studies and analysis principles. Different indicators and metrics will be defined to comprehensively assess the levels of digitalisation and cybersecurity in both countries considering the existing information sources. The study's research findings and analysis are supplemented by findings from several expert workshops. These workshops were conducted with representatives from various actors in the energy sector, including grid operators, energy suppliers, system providers, regulators and ministries.

A detailed description of the study contents will be given in Section 1.5.

1.2 German-Israeli Energy Partnership

The German-Israeli Energy Partnership was initiated by both governments in early 2022 to enhance and broaden the collaboration between Germany and Israel. It serves as a foundation for the energy and climate security in both nations and presents significant learning potential regarding the energy transition and cybersecurity of critical energy infrastructures. The partnership includes a range of joint activities, including workshops, research studies, conferences and delegation trips. It is divided into two working groups that act as advisory bodies, organised by the Israeli Ministry of Energy and Infrastructure (MoE), the German Federal Ministry for Economic Affairs and Climate Action (BMWK), the Federal Ministry of the Interior, Building, and Community (BMI), and the Israel National Cyber Directorate (INCD).

The first working group *Energy Policy Issues* (EPI) is organised by the MoE and the BMWK. Its goals include:

- accelerating the development of efficient and affordable systems for hydrogen storage, transport and conversion;
- increasing the capacity of energy grids and infrastructure to generate, store and utilise renewable energies;
- enhancing existing buildings and using energy-efficient materials in new constructions;
- and developing physical submarine gas infrastructure.

The second working group *Digitalisation and Protection of Critical Energy Infrastructure* (DPCE) is organised by the MoE, BMWK, BMI and INCD. This group focuses on cooperation in the fields of digitalisation and protection of critical energy infrastructures. It aims to share knowledge to increase resilience against cybersecurity incidents in critical energy infrastructures by establishing best practices, developing suitable security standards and fostering research.

The working programme is implemented by the German Energy Agency (dena) to support the activities of the partnership and to achieve the common goals.[1]

1.3 Areas of interest

The areas of interest guide the study's research and analysis work and reflect the current and near-future developments in the energy sectors in Germany and Israel. They focus on key aspects of how the ongoing use of digital technologies and the increased threat of cyber-attacks affect the relevant actors and systems in the electrical energy supply. These aspects encompass the ongoing integration of renewable energies and system flexibilities, recent advancements in smart metering systems and energy markets as well as the state of communication and level of expansion in transmission and distribution systems. The following areas of interests will be considered throughout the study:

1. Integration of small and medium-sized power producers (e.g., photovoltaic roof systems or wind power plants), ensuring an efficient management of distributed energy sources;
2. Smart metering systems allowing real-time monitoring and empowering consumers with direct access to energy data;
3. Liberalised energy markets and market communication, facilitating an efficient and transparent data exchange and transactions for business models;
4. Transmission and distribution system and the state of associated digitalised supervision and grid expansion measures for a stable and efficient operation and control of the power system.

1.4 Source material

To achieve the study's goals, a sufficient number of up-to-date and representative information sources should be available for both the German and Israeli energy sector. Especially for Israel, there exist information gaps resulting from:

- non-public or classified information about sector-specific regulations and security controls;
- missing or outdated information regarding strategic documents in digitalisation and cybersecurity;
- information about stakeholders, ownerships, system operators and regulators being unavailable; and
- scarcity of publicly available studies and surveys from industry or associations.

In particular, the last point serves to protect national security interests but impedes research efforts and the development of informed policy recommendations.

[1] Israel Energy Partnership (2025)

These circumstances make it difficult to take a holistic view of the energy sector in Israel and to fully and comprehensively compare both countries in all aspects of digitalisation and cybersecurity. Despite this, this study aims to present a balanced and multifaceted comparative analysis regarding the current states and recent developments in the German and Israeli energy sectors.

1.5 Study outline

Chapter 1: 'Introduction' presents the study's objectives and areas of interest. Chapter 2: 'Fundamentals' introduces basic technical aspects and general developments in digitalised electrical energy systems, liberalised energy markets and cybersecurity. This should most of all help non-experts to better understand the investigations and insights given in the subsequent chapters. Furthermore, Chapter 3: 'Initial situation' briefly describes and compares the initial situations in Germany and Israel, including the national grand strategies as well as their respective energy infrastructure and main actors. These findings will serve as a starting point for the further in-depth analysis of the state of digitalisation and cybersecurity of both countries in Chapter 4 and Chapter 5.

The 'state of digitalisation' in the energy sectors of Germany and Israel is presented in Chapter 4. Following the areas of interest of this study (see Section 1.3), the analysis encompasses a comprehensive view of energy market roles and business models, smart metering systems, installations of distributed energy producers, including renewable energies, and the transmission and distribution systems in the energy sector. Finally, a set of indicators and quantitative metrics will be derived reflecting the digital advancements in the context of system efficiency, sustainability and market competitiveness in both countries.

The 'state of cybersecurity' in the energy sectors of Germany and Israel is presented in Chapter 5. In step one, the study describes the cybersecurity architectures by reviewing the regulating authorities, non-governmental institutions and contact points. In step two, the cyber threat situation in the energy sectors will be analysed according to the areas of interest of this study (see Section 1.3). Finally, a set of indicators and qualitative metrics will be derived reflecting the tasks of authorities and institutions as well as the criticality of relevant cyber threats and corresponding systemic weaknesses in both countries.

Taking the results from Chapter 4 and Chapter 5, the 'comparative analysis' in Chapter 6 summarises the main similarities and differences in the digitalisation efforts as well as the cybersecurity architecture and cyber threat situation between the German and Israeli energy sectors. In conclusion, the chapter highlights key areas of common innovations and their associated benefits based on the identified challenges and inhibitors of digital advancements and cybersecurity efforts, considering the unique political and economic conditions in each country.

Chapter 7: 'Recommended actions' outlines regulatory, process and technological recommendations and suggests potential future projects from identified common innovation fields for the energy sectors in Germany and Israel. A final summary of the study's main findings regarding the comparative analysis of the German and Israeli energy sectors as well as the resulting innovation fields and recommended actions is provided in Chapter 8: 'Conclusion and summary'.

2 Fundamentals

The electrical energy sector is undergoing a significant transformation driven by the integration of renewable energy, market liberalisation and technological advancements such as IT/OT convergence and smart grid technologies. This evolution is complemented by the adoption of system flexibilities such as energy storage systems, demand response programs and electric vehicles to ensure grid stability. Additionally, the increasing occurrence of cyber-attacks on critical infrastructures underscores the urgent need for robust cybersecurity measures.

For a comprehensive understanding of this study, this chapter introduces the most relevant technical fundamentals regarding digitalisation and cybersecurity in the electrical energy sector. This includes descriptions of:

- the general architecture and automation processes in the electrical energy sector in Section 2.1;
- the major digitalisation drivers through the integration of renewable energy sources, liberalised energy markets, smart metering and the ongoing IT/OT convergence in Section 2.2; and
- the relevant cybersecurity aspects and cyber threats in ICS environments in Section 2.3.

2.1 Electrical energy sector

The energy sector is vital for modern society, supporting critical systems like healthcare, transportation and ICT, while its ongoing transition to renewable energy and advanced technologies presents both opportunities and challenges. Meeting growing power demands and achieving net-zero emissions by 2050 requires substantial investments in smart grids, infrastructure and renewable energy expansion. These goals, agreed upon by nearly 200 countries at COP28[2], aim to transform the global energy sector and mitigate climate change impacts[3]. However, the path to a more resilient and sustainable energy grid is fraught with challenges. The need for modernisation, substantial financial investments and effective coordination among stakeholders is critical[4]. For example, the power sector is confronting with tremendous challenges, including the growing frequency of extreme weather events and the necessity to make progress on the green transition. This transformation requires integrating power generation, transmission and distribution into smart grids managed by digital systems and artificial intelligence[5].

System architecture: from transmission to distribution

The electrical energy system relies on key components and actors, with energy producers generating electricity that is transported via transmission and distribution systems to consumers[6]. TSOs manage high-voltage grids, ensuring grid security by balancing electricity, regulating frequency, maintaining reserves for outages and providing black start capabilities for emergencies[7,8]. While transmission systems are highly automated for real-time operation, DSOs manage less-automated, lower-voltage grids, addressing local overloads and delivering electricity to end-users[9,10]. Figure 1 illustrates electricity distribution from high-voltage power lines through substations that reduce voltage levels, ultimately delivering power to industrial users, corporations and households via local distribution systems[11].

[2] Bundesregierung (2025)
[3] Spence (2024)
[4] IEA (2025a)
[5] Nature (2023)
[6] Poudineh et al. (2022)
[7] Csanyi (2017)
[8] ENTSO-E (2015a)
[9] Technology (2013)
[10] ENTSO-E (2015b)
[11] Pansini (2005)

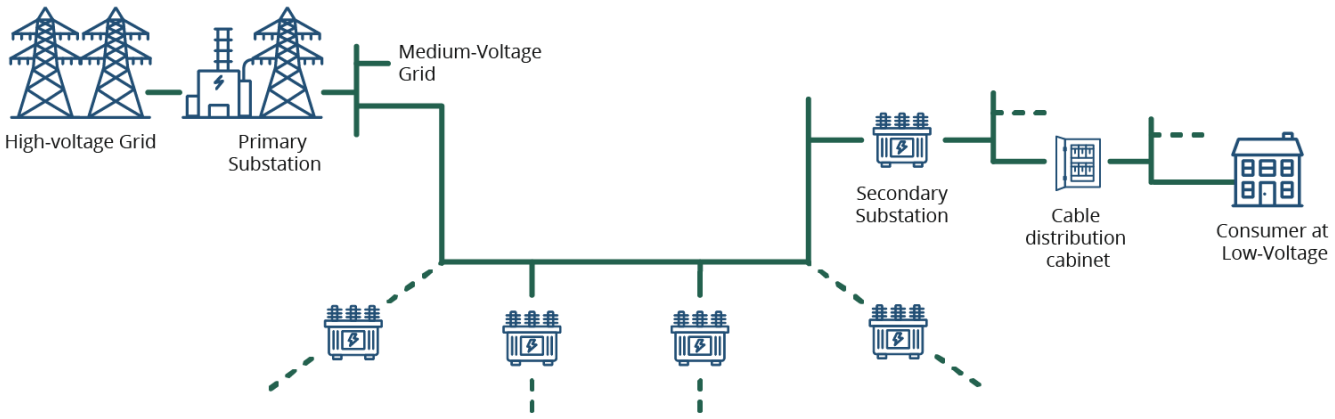


Figure 1: Simplified illustration of a medium-voltage grid

Automation levels: from process control to grid control

Electrical energy systems are managed through a hierarchical structure using advanced automation. At the enterprise level, business processes like billing and customer service are supported by information technology (IT), which handles data processing, storage and communication. Below this is the ICS (industrial control systems) level, which includes operational technology (OT) — hardware and software that directly control physical processes such as power plant operations and electricity flow — and SCADA systems for monitoring and control. The OT-DMZ secures communication between business and industrial networks.[12, 13] At the process control level, the hierarchy reaches the physical components of the system, such as sensors, actuators and programmable logic controllers (PLCs), which directly manage electricity flow and ensure grid stability.

[12] Sakai et al. (2022)

[13] INCIBE (2025))

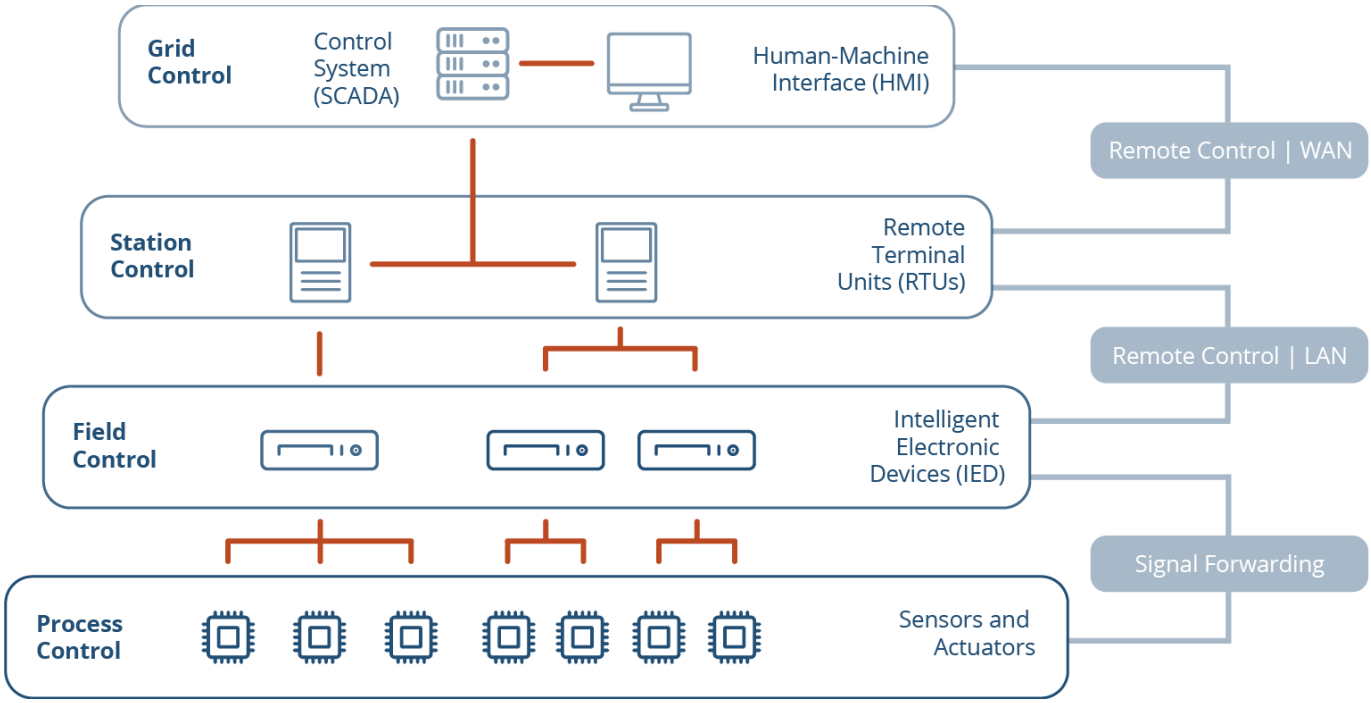


Figure 2: Simplified illustration of power grid control architecture[14]

Figure 2 illustrates the different levels of control in a modern electrical grid, each playing a specific role in managing and ensuring the smooth operation of the power system. Here's an explanation of the key terms used in the diagram:

1. *Grid control*: Operators use SCADA systems to manage electricity flows in real time, with human-machine interfaces (HMI) providing visual tools for decision-making. Communication relies on wide area networks (WAN) to connect grid components over large distances.
2. *Station control*: Local control occurs at substations, where high-voltage electricity is transformed for distribution. Remote terminal units (RTUs) at these substations report status updates and execute grid control commands, communicating over local area networks (LAN).
3. *Field control*: Intelligent electronic devices (IEDs) monitor and manage field equipment, autonomously responding to faults or surges and relaying critical data to higher control levels.
4. *Process control*: Sensors measure conditions like voltage and current, while actuators control equipment such as switches and transformers. Data from this level informs upper systems, ensuring grid stability and performance.

This hierarchical system ensures that the grid is monitored and managed efficiently, from the central control down to the actual physical processes that generate and distribute electricity. Each level communicates in a vertically oriented hierarchical structure, aggregating lower-level information and transmitting only relevant and urgent data upward to enable quick issue resolution and maintain the balance of power supply and demand across the grid.[15]

[14] Stoupis et al. (2023)
[15] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2024)

2.2 Digitalisation: from renewables to smart meters

The energy sector is undergoing rapid transformation, driven by the integration of renewable energy, the liberalisation of energy markets and technological advancements like IT/OT convergence[16]. While these changes offer significant opportunities for improving efficiency and sustainability, they also present new challenges, particularly in terms of managing grid stability, ensuring cybersecurity and adapting to the growing complexity of the energy system[17].

Renewable energy sources and system flexibilities

One of the most significant changes in the energy sector is the growing integration of RESs such as solar and wind power. These sources are clean and sustainable, but they can be unpredictable, as solar power varies both seasonally and can be affected by cloud coverage, and wind power depends on wind conditions. To manage this variability, system flexibilities such as energy storage systems (or batteries), demand response (DR) programmes (which encourage consumers to reduce energy use during peak times) and electric vehicles (EVs) (which can also be used as energy storage) are becoming increasingly important[18]. These technologies help to balance the energy supply and demand and ensure a stable grid operation in case of fluctuating renewable energy production[19].

Liberalised energy market and smart meters

The energy market has been opened to competition, allowing multiple stakeholders to participate in trading energy. Platforms like the European Energy Exchange (EEX) and EPEX/Spot enable energy producers, suppliers and buyers to trade electricity[20]. A key aspect of this system is the formation of balancing groups that ensure the amounts of energy produced and consumed match at every time point. This requires effective market communication between these stakeholders[21].

Another critical innovation is smart metering, a technology that allows both consumers and energy providers to monitor the electricity usage in real time[22]. Smart metering systems are becoming essential tools in modernising energy infrastructures worldwide. These systems enable a detailed tracking of energy consumption and offer real-time data to aid demand-side management, grid stability and energy efficiency improvements. By providing consumers and grid operators with actionable insights, smart meters help to optimise energy usage patterns, reduce peak demands and integrate renewable energy sources more effectively[23]. Additionally, smart meters facilitate two-way communication between energy providers and consumers, paving the way for advanced functionalities like dynamic pricing, demand response and integration with decentralised energy resources[24]. While smart metering solutions depend on local regulations and infrastructures, the core benefits of enhanced transparency, improved billing accuracy and the support of energy transition efforts are universal, making them valuable assets for energy systems aiming for sustainability and resilience[25].

Convergence of IT and OT systems

A major trend reshaping the energy sector is the convergence of IT and OT. While IT is traditionally used for managing data and communication systems (like computers and servers), OT is used for controlling physical processes (like the operation of machinery in power plants). The merging of these two areas, known as IT/OT convergence, allows for more advanced monitoring and control of energy systems. Figure 3 illustrates the layered structure of energy systems, with applications such as wind parks, smart metering and public charging infrastructure at the top, supported by underlying infrastructures like SCADA systems, cloud infrastructure and the convergence of IT and OT systems[26].

[16] Tata Consultancy Services (2025)
[17] IEEE Smart Grid (2025)
[18] Courier Mail (2024)
[19] Yazdandoust and Golkar (2020)
[20] ENTSO-E (2024)
[21] Next Kraftwerke (2025)
[22] IBM (2025)
[23] Fraunhofer Institute for Solar Energy Systems ISE (2025c)
[24] Nhede (2019)
[25] Clou (2023)
[26] Dhlamini and Mawela (2022)

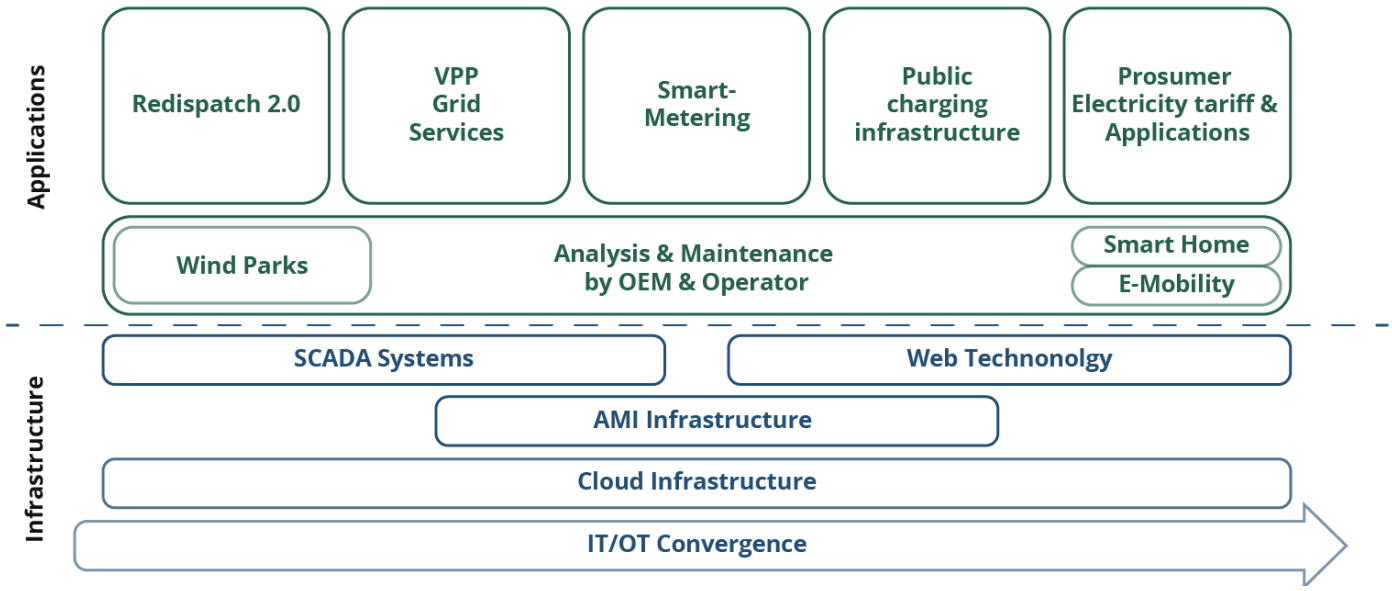


Figure 3: Schematic illustration of the ongoing process of IT and OT convergence in smart grids[27]

It highlights the integration of digital technologies to manage and optimise energy services, particularly focusing on smart grid services, e-mobility and prosumer participation in the energy market. This means that technologies like cloud services (where data is stored and processed online), virtualisation (where physical devices are replaced by virtual ones) and wireless networks are increasingly being used to make the energy grid more efficient and flexible. However, this convergence also brings new risks, particularly in terms of cybersecurity, as integrating IT and OT systems creates potential new vulnerabilities[28].

2.3 Cybersecurity and cyber threats

The energy sector faces increasing threats from cybercrime, with industrial ransomware attacks, supply chain attacks and denial-of-service (DoS) attacks becoming more prevalent in ICS environments. These cyber threats pose significant risks to the reliability and safety of critical infrastructure systems and components, highlighting the ongoing need for effective cybersecurity measures and controls. Especially in the energy sector, cyber-attacks can lead to severe consequences for the energy supply at the transmission and distribution level.

CIA triad and OT security

Cybersecurity is a subfield of information security that focuses on the protection of digital (cyber) information against cyber threats. Information security is concerned with the protection of information and the mitigation of security risks in software and hardware components as well as in communication networks. It addresses the secure handling of information at a physical, personal and organisational level. The core aim of information security is to ensure the confidentiality, integrity and availability of information (also known as the CIA triad[29]):

- *Confidentiality* aims to prevent unauthorised access to information. It ensures that sensitive information is accessible only to those who are authorised to view it (e.g., by way of encryption or two-factor authentication).
- *Integrity* involves maintaining the completeness and correctness of information. It ensures that data is accurate and has not been tampered with or altered in unauthorised ways (e.g., via digital signatures).
- *Availability* ensures that information is readily accessible to authorised users when needed. It involves maintaining the functionality of systems that store, process and transmit information (e.g., via firewalls or recovery plans).

[27] Energy Gov (2025)
[28] Bundesamt für Sicherheit in der Informationstechnik (2024)
[29] Fortinet (2025)

In the context of the ongoing IT/OT convergence in the electrical energy sector (see previous section), the traditional primitives of IT security are not appropriate for the protection of OT systems. *OT security* follows a different prioritisation compared to the CIA triad and mainly strives for availability as the primary protection goal (also referred to as the 'AIC' triad). Alternative frameworks for OT security define safety, reliability and availability (SRA) as primary security goals. A comparison of the protection goals of IT and OT security is shown in Figure 4

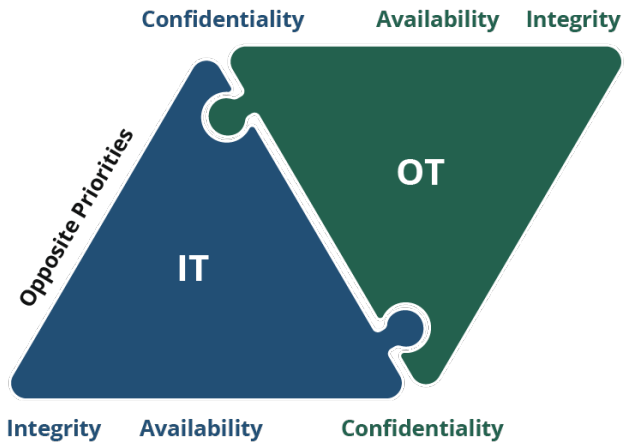


Figure 4: IT security vs. OT security protection goals[30]

At the field level, OT systems exhibit direct physical effects, including complex interactions with physical processes. Hence, maintaining operational safety is highly important when implementing security measures and represents an additional major challenge compared to IT systems. OT systems are characterised by time-critical and continuous processes with very low acceptance of disruptions or outages, which places special demands on performance and reliability. Also, the high resource constraints of OT systems, which often operate in isolated remote locations, limit the capabilities to implement proper cybersecurity measures. The use of legacy hardware or software components complicates the implementation of security patches, and the strong presence of monopoly providers leads to high risks of common cause failures.[31, 32, 33, 34, 35]

ICS Cyber Kill Chain model

A cyber threat is a potential risk of exploitation of a vulnerability in a computer system or a communication network. Cyber threats are posed by a threat actor (individual, group or organisation) with malicious intent, thereby triggering a cyber-attack at a selected target. This leads to a cyber incident, causing potential harm such as data breaches, financial loss and damage to or malfunctioning of systems. The SANS Institute introduced the ICS Cyber Kill Chain model[36] to describe the general phases of cyber-attacks in ICS environments; it is based on the general Cyber Kill Chain model from Lockheed Martin[37]. The ICS Cyber Kill Chain model is divided into the two main phases:

- cyber intrusion preparation and execution (phase 1); and
- ICS attack development and execution (phase 2).

[30] Tesco Controls (2025)
[31] Pfendler et al. (2022)
[32] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2024)
[33] Schwarz (2023)
[34] William Knowles et al. (2015)
[35] Stouffer et al. (2023)
[36] Assante and Lee (2015)
[37] Lockheed Martin (2025)

In phase 1 (see Figure 5), the attacker gains access to information to target, deliver and exploit elements of the ICS target system. This includes performing reconnaissance to identify technical vulnerabilities and other possible exploitations of the process and operating model. Based on this, the attacker identifies exploitable victims in the target system (targeting) and prepares the corresponding attack tools (weaponisation). In the cyber intrusion step, the attacker gains initial access (e.g., by delivering a phishing e-mail), performs a malicious activity (exploitation) and installs or modifies a capacity (e.g., via a remote access Trojan). In the final management and enablement step, the attacker establishes a command and control (C2, or C&C) server to perform further actions, including the discovery of new systems, lateral movements, launching of new capabilities, capturing of transmitted communications, data exfiltration or applying anti-forensic techniques.

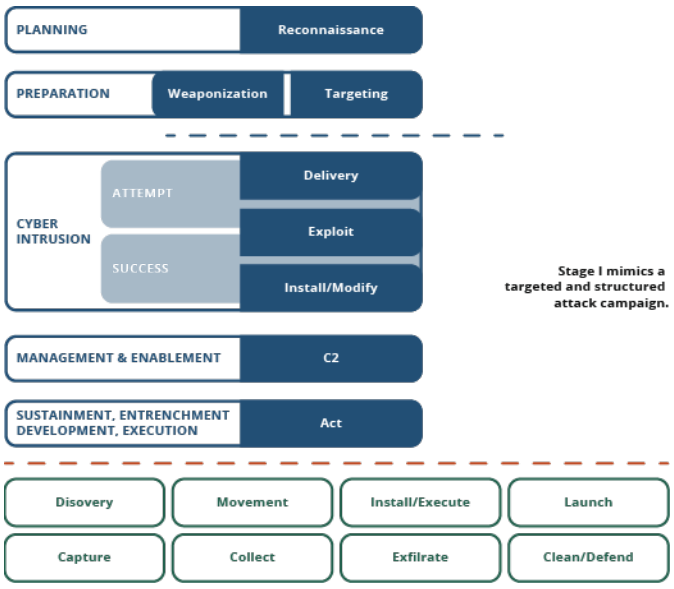


Figure 5: The ICS Cyber Kill Chain model: phase 1[38]

Phase 2 (see Figure 6) involves the execution of the intentional cyber-attack on the ICS target system using the knowledge gained from phase 1. In the attack development and tuning step, the attacker develops new capabilities tailored to specific ICS components using exfiltrated data. In the validation step, the attacker tests these capabilities, including the acquisition of physical ICS components and their software.

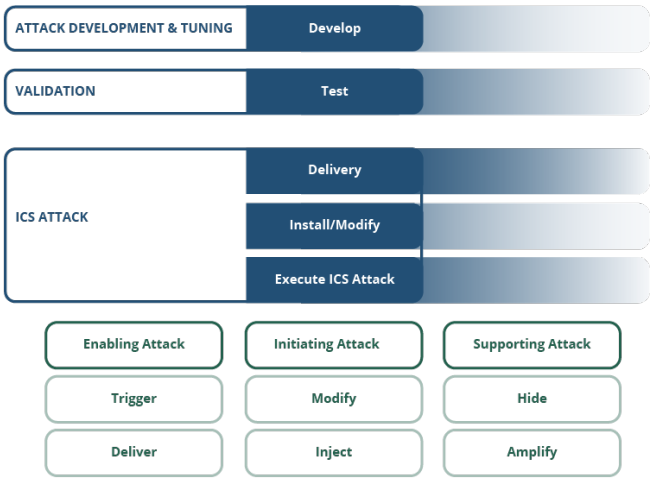


Figure 6: The ICS Cyber Kill Chain model: phase 2[38]

Based on this, the attacker finally delivers the capability on the target system and executes the cyber-attack (e.g., to manipulate process elements or set points, spoof state information). The most common attack objectives in ICS environments include:

- loss of views or controls;
- denial of views, controls or safety; and
- manipulation of views, controls, sensors or safety.

[38] Assante and Lee (2015)

From ENISA prime threats to cyber threats in critical infrastructures

The European Union Agency for Cybersecurity (ENISA) publishes a yearly report on the most relevant cyber threats (primal cyber threats) and their trends in the public and private sector. From the years 2021[39] and 2023[40], ransomware attacks were identified as primal threats, followed by malware and denial-of-service attacks. Ransomware attacks (e.g., WannaCry[41] or CrypoLocker[42]) are used to take control of critical assets (e.g., databases) and demand ransom to regain access. They are often triggered by phishing e-mails and increasingly target cloud infrastructures. Malware attacks (e.g., via computer viruses, Trojans or worms) inject malicious code into devices to execute unauthorised processes. The biggest threat presented by malware attacks involves data theft (e.g., Agent Tesla[43] or Redline Stealer[44]). They focus more on container environments and pose a high risk for supply chains or service providers (by introducing 'backdoors'). DoS attacks overload system resources or services to put them out of operation. They focus more towards mobile networks and IoT devices; ransom DoS attacks are identified as a new emerging threat. Other relevant cyber threats increasingly use AI assistance for social engineering and the compromise of business e-mails.

Also, these threats can significantly impact OT systems and components in critical infrastructures like the electrical energy sector. Here, attackers infiltrate their targets at the enterprise level or via other peripheral systems to further propagate to the OT systems. This includes industrial ransomware-as-a-service (RaaS) attacks on OT devices or the infection of OT devices with malware products via mobile devices or from the public Internet. Examples include incidents at a German nuclear power plant in 2016[45] involving the use of USB flash drives as well as incidents at Australian energy provider Integral Energy in 2009[46]. Compromised firmware updates (e.g., within supply chains or by attacking software providers) in power plants, generation units or other assets in particular allow for the placement of 'backdoors' (e.g., to manipulate control units) and remain undetected for long periods of time. For example, this cyber threat has been reported by the US Department of Defence in relation to Lenovo microcomputers. DoS attacks are seen as major upcoming threat for wireless communication networks. Additionally, the compromise of business e-mails or the dispatch of phishing e-mails via social engineering at the enterprise level of critical infrastructure companies are still seen as a major entry point for cyber-attacks.[39, 40, 47]

Supply chain attacks in ICS environments

Manufacturers and vendors are pivotal in ICS environments (e.g., in the energy sector). Large multi-national companies (MNCs) wield significant influence, shaping industry standards and driving technological advancements. Meanwhile, small and medium-sized enterprises (SMEs) rely heavily on these external providers to access essential technologies and remain competitive in the market. These manufacturers and vendors are increasingly confronted with supply chain attacks, which exploit the relationship of trust from customers and can remain undetected for long periods of time. Figure 7 illustrates the supply chain model in common ICS environments, including the relevant actors and their responsibilities.

[39] Lella et al. (2021)
[40] Ardagna et al. (2023)
[41] MITRE ATT&CK (2024a)
[42] Kapersky (2025)
[43] MITRE ATT&CK (2024b)
[44] FKIE (2025c)
[45] Trend Micro (2025)
[46] SPAMfighter (2025)
[47] Böswetter et al. (2021)

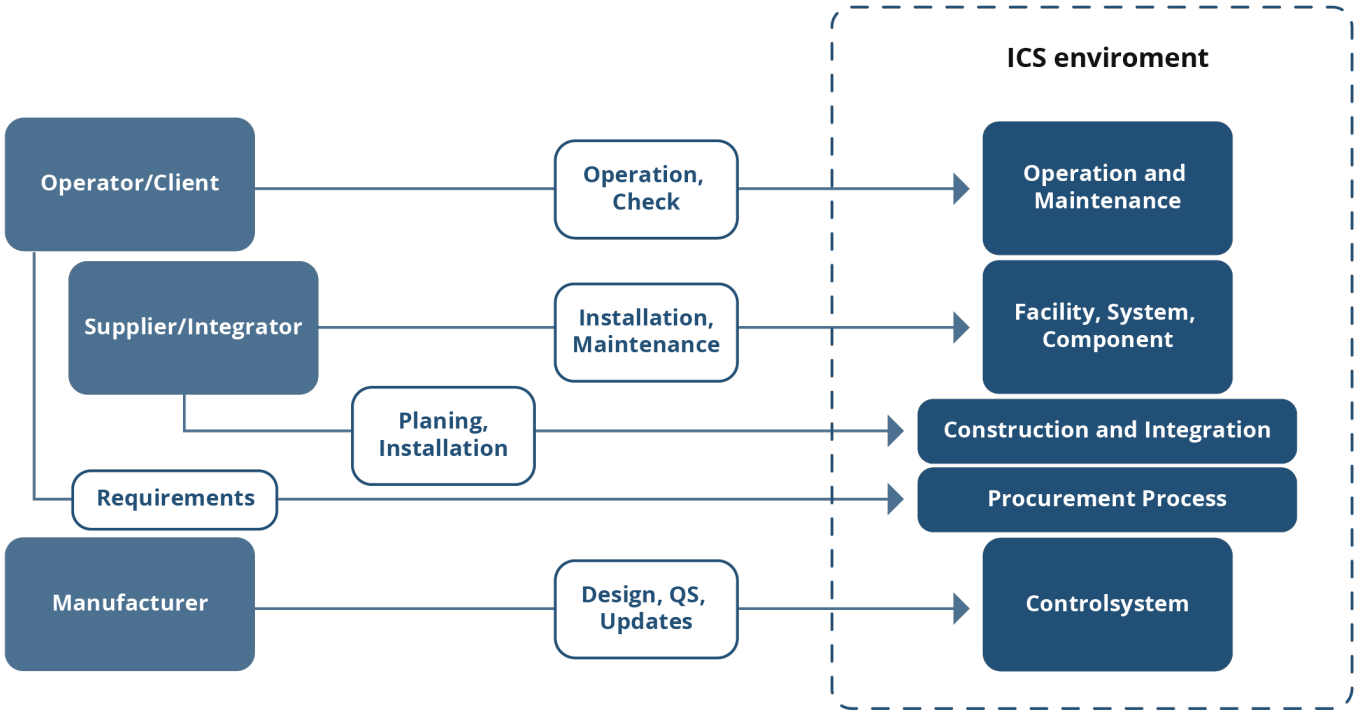


Figure 7: Supply chain model in ICS environments (adapted)[48]

Manufacturers develop hardware and software products, ensuring quality standards and implementing corresponding security tests and updates, whereas the system and plant operators define the necessary cybersecurity measures and controls. Integrators carry out site acceptance and integration tests with operators and manufacturers in compliance with defined cybersecurity requirements. Successful attacks on supply chains (e.g., by manipulating maintenance or operating system software) can lead to severe and large-scale system damages affecting a large number of operators and suppliers.[48, 49, 50]

As a prominent example, from April to June 2022 the threat group Red Ladon ran a cyber espionage campaign against different MNCs, including supply chains of offshore wind energy projects, in the South China Sea. The threat group especially targeted manufacturers that are responsible for the maintenance and installation of offshore wind farms. They used phishing e-mails and posed as a fictional media company to deliver a ScanBox malware to the victims.[51]

[48] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2024)
[49] Lella et al. (2021)
[50] Ardagna et al. (2023)
[51] Proofpoint (2022)

3 Initial situation in Germany and Israel

As outlined at the start of Section 2.1, the energy infrastructure operates hierarchically: high-voltage transmission transports bulk energy from large producers (conventional power plants, large wind farms), branching into medium-voltage distribution on a regional level (smaller scale wind farms or large solar producers as well as large industrial consumers), down to a local level, where low-voltage power lines deliver electrical energy to highly dispersed end consumers.

Historically, both Germany and Israel have followed this approach throughout the last century and are now transitioning towards a more dynamic infrastructure which must account for large quantities of energy production by RESs in the lower-voltage grids. Differences in the two systems arise from the size of the area being serviced in both countries, the mix of energy resources utilised and cooperation with or threats stemming from adjacent countries and territories.

This chapter describes the initial situation of the electrical energy sector in Germany and Israel, also considering the political agenda and the regulatory framework:

- Section 3.1 introduces the digitalisation and cybersecurity strategy, describes the electrical infrastructure and its connections to neighbouring countries and highlights the relevant regulatory authorities.
- Section 3.2 summarises the main facts from Section 3.1 regarding the general infrastructure, ownership and coordination as well as the regulatory bodies responsible from a governmental standpoint.

3.1 Grand strategy, infrastructure and regulation

3.1.1 Geographic and political background

Germany

Germany's strategic location at the heart of Europe makes it a key geographic and political hub, deeply interconnected with its neighbours. Sharing borders with nine countries — Denmark, Poland, the Czech Republic, Austria, Switzerland, France, Luxembourg, Belgium and the Netherlands — it serves as a critical corridor for trade, transport and energy flows. Its access to the North and Baltic Seas further enhances its global connectivity via maritime trade. Politically, Germany is a federal parliamentary republic with 16 states, each with its own government, fostering regional governance alongside a strong central administration. Berlin, its capital, is a major cultural and political hub, hosting international organisations and embassies. As a founding member of the European Union (EU), Germany wields significant influence in EU policymaking, particularly on energy, climate change and digitalisation. It is also a member of the United Nations, NATO, the G7 and the G20, underscoring its global importance.[52]

Germany's role in the trans-European electricity grid highlights its importance in regional energy security. As a member of the European Network of Transmission System Operators for Electricity (ENTSO-E), Germany contributes to grid stability through cross-border electricity trading and renewable energy integration. ENTSO-E ensures the efficient operation of Europe's electricity grid and balances electrical energy production and consumption across the countries borders, thus promoting grid stability and supply security.[53]

[52] Grotz and Schroeder (2023)

[53] ENTSO-E (2025)

Israel

Israel has faced critical threats to its national security since its establishment, contending with adversaries ranging from hostile states like Iran and Lebanon to failed states such as Syria and state-like entities like Hamas and Hezbollah. In response, Israel is expanding its defence strategy from traditional military capabilities to a focus on the cyber domain, acknowledging the evolving nature of warfare. Geographically isolated, Israel operates as a 'desert island', making it imperative to develop independent infrastructures and not rely on neighbouring countries. A project aiming to connect Israel to the Cypriot grid via undersea power cable has commenced according to the Israel Electric Corporation (IEC) as a possible means of feeding excess electricity from renewable sources in Israel into the European grid. Additional options of connecting Jordan and Egypt are also being considered.[54]

The Ministry of Energy and Infrastructure (MoE) is actively promoting a diverse energy supply, including the development of its natural gas sector, fuel imports and renewable energy production. Additionally, the MoE emphasises energy savings and efficiency to enhance resilience.[55, 56, 57]

The special situation in Israel has been further exacerbated since the onset of Operation Iron Swords in 2023, which has intensified the existing challenges and underscored the urgency for a robust and adaptable national security strategy. This marks a significant escalation in Israel's ongoing conflict with militant groups, primarily Hamas and Hezbollah. The operation was initiated in response to a series of coordinated attacks targeting Israeli civilians and military installations, which have raised alarms about the security landscape in the region.[58]

3.1.2 Grid infrastructure

Germany

Germany's digitalisation efforts are heavily driven by the Energiewende (energy transition), a national initiative focusing on a shift from fossil fuels to renewable energy sources such as wind and solar[59]. In 2024, renewables accounted for a substantial share (57 per cent) of Germany's net electricity production. This transition has led to challenges in grid management due to the intermittent nature of renewable energy, necessitating upgrades to infrastructure and the deployment of technologies like smart grids to ensure stability and efficient energy flow. Germany's energy infrastructure includes a diverse mix of public and private ownership.

On the transmission level, Germany's energy system is divided into four control areas, each managed by a different TSO: 50Hertz, Amprion, TenneT and TransnetBW.

These TSOs are responsible for balancing electricity generation and demand within their regions. Energy from the transmission system (usually running at 380/220 kV) is then transformed to 110 kV at transformer stations where initial distribution to consumers begins. This marks the point at which larger DSOs assume control. Apart from large industrial consumers, these high-voltage levels often accommodate feed-in from medium-sized power plants, mostly conventional or hydropower plants. Further transformation takes place at regional distribution grids operating at levels such as 30 kV, 20 kV or 10 kV. These grids accommodate industrial consumers along with large-scale RES installations and energy storage systems. The final grid level is achieved at 0.4 kV (400 V) where small substations distribute electrical energy along branched or meshed lines to small businesses and households. This traditionally one-way distribution is being challenged by the rise of small-scale RESs (rooftop solar) feeding into the system.

[54] Gov IL (2024a)
[55] Gov IL (2024b)
[56] Frei (2020)
[57] Mizrahi et al. (2024)
[58] Israel National Cyber Directorate (2024a)
[59] Bayer (2015)

The transmission grids are largely managed by private TSOs, while many smaller, local energy providers and renewable energy installations are owned by municipalities, cooperatives and private companies. This mixture of ownership requires coordinated regulatory oversight to ensure effective competition, fair access and reliable grid management. The decentralised structure is designed to efficiently accommodate a growing variety of energy sources, particularly renewables, ensuring stability across the grid. This decentralisation is a critical feature in managing regional energy needs and integrating renewable energy into the system.

Israel

From Israel's founding in 1948 until the early 21st century, the Israeli electricity sector was almost exclusively dominated by the IEC. It wasn't until 2007 that the government introduced a policy, known as the First Reform, which set the stage for competition with the IEC, specifically in the generation and supply segments. In 2011, the government launched the Second Reform, aimed at boosting renewable energies in the sector by encouraging the involvement of entities other than the IEC. A third reform was introduced in 2018, targeting the restructuring of the IEC to focus solely on transmission and distribution. While ownership of the transmission and distribution grids remains with the IEC, the 2018 reform saw the creation of the independent system operator (ISO) Noga – Electricity System Management Ltd., a government-owned entity, which is tasked with electricity supply management, market operations, emergency preparedness and fuel switching. As part of the electricity reform, Noga facilitates the switching of consumers from the IEC to private electricity suppliers, aiming to increase competition and efficiency in the market. [60, 61, 62]

The transmission and distribution systems are owned, operated and maintained by the IEC and operate at ultra-high (400 kV) or high voltage (115, 161 kV). Apart from large industrial consumers, these high- to medium-voltage levels accommodate feed-in from large to medium-sized power plants, such as conventional gas-fired power stations. Transformation takes place at regional distribution grids operating at levels such as 13 kV, 22 kV or 33 kV. These grids accommodate industrial consumers along with large-scale RES installations and energy storage systems. The final grid level is reached at 0.4 kV (400 V) where small substations distribute electrical energy along branched or meshed lines to small businesses and households.

3.1.3 Regulation

Germany

The Federal Office for Information Security (BSI) operates under the Federal Ministry of the Interior and Community (BMI) as Germany's national cybersecurity agency. Its role in securing critical infrastructures, including the energy sector, was strengthened by the second German IT Security Act (IT-SiG 2.0). The BSI's responsibilities include the prevention, detection and response to cyber threats, and it serves as the central body for cybersecurity certification and standardisation. The BSI plays an important role in protecting both government agencies and digital consumers in the energy sector.[63]

The Federal Network Agency (BNetzA), under the Federal Ministry for Economic Affairs and Climate Action (BMWK), regulates Germany's energy, telecommunications, postal services and railway sectors. In the energy sector, the BNetzA ensures fair access to the electricity and gas grids, regulates grid charges and sets market conditions to promote competition. It also enforces cybersecurity measures and supervises the secure operation of the grid. The BNetzA is essential in maintaining the transparency and integrity of the energy market in Germany.[64]

[60] Julian (2021)
[61] Avri Eitan (2023)
[62] Elmas (2024)
[63] Bundesamt für Sicherheit in der Informationstechnik (2023a)
[64] Bundesnetzagentur (2024)

Israel

The Ministry of Energy and Infrastructure (MoE) implements policies and creates the regulatory infrastructure to guarantee the electricity, water and gas supply in routine and emergency cases. The MoE regulates privately-owned energy producers, the energy market, and protects consumers. It also develops expertise at a staff level at the ministry.[65]

The Israel Public Utility Authority for Electricity (PUA), also referred as 'The Electrical Authority', regulates and supervises the public utilities in the electrical energy sector to balance the interests of consumers, the IEC, private bodies and the state. This includes the setting of production and electricity rates as well as indicators for the quality of services.[66, 67]

The Israel National Cyber Directorate (INCD) under the Prime Minister's office was established in 2017 (government resolutions 2444 from February 2015 and 3270 from December 2017) following the merger of the National Cyber Security Authority (NCSA) and the Israeli National Cyber Bureau (INCB). The INCD is the national security and technological agency in charge of defending Israel's cyber space and organises the civilian cybersecurity landscape.[68, 69]

3.1.4 Digitalisation strategy

Germany

The digital strategy for Germany (published in August 2022[7071]) is an overall framework for digital policies up to the year 2025 involving several federal ministries (e.g., BMI, BMWK) and is coordinated by the Federal Ministry for Digital and Transport (BMDV). It aims to enhance competences in pivotal technologies such as software development, microchips, sensors, artificial intelligence, quantum computing and communication technologies. By 2025, the strategy targets significant milestones including equipping 50 per cent of all stationary connections with fibre optic lines, ensuring the nationwide availability of wireless voice and data services, enhancing the utilisation of data spaces and aiding small and medium-sized enterprises (SMEs) in adopting artificial intelligence applications and data-driven business models. The relevant fields of action of the digital strategy include:

1. *Digital infrastructures* to ensure a comprehensive, energy, and resource-efficient supply of fiber optic connections to support digital connectivity,
2. *Mobility* to accelerate the market introduction of electric vehicles by expanding the charging infrastructure,
3. *Data economy* to establish robust data infrastructures such as data platforms and data spaces (e.g., Gaia-X) across various sectors to foster a data-driven economy, and
4. *Climate and resources* to develop legal frameworks and standards for intelligent measuring systems (smart meters) with a strong emphasis on cybersecurity.

[65] Gov IL (2024b)
[66] Gov IL (2024c)
[67] Shakhak (2023)
[68] Frei (2020)
[69] Tabansky (2020)
[70] Bundesregierung (2024)
[71] Digitalstrategie Deutschland (2024)

Israel

Israel is known as a start-up nation and stands out as a leading technological innovator, fostering a dynamic ecosystem for technology and entrepreneurship. In 2017, the Digital Israel Bureau within the Ministry for Social Equality launched the National Digital Programme, which reflects the government's policy agenda up to 2020. The primary goals of this strategy include:

- *Reduction of socio-economic gaps* to bring the geographic and social periphery closer and to reduce living costs;
- *Acceleration of economic growth* to advance digital industries and businesses, to shift the employment market into the digital age and to support infrastructure development; and
- *Smart and friendly government* to improve the accessibility to national and local government, to promote an innovative and effective government and to improve public goods.

Implementation areas for these initiatives encompass local government, economics and finance, housing and real estate, law, health, employment and social services, as well as schooling and education. Ultimately, the vision is to leverage the opportunities presented by the digital revolution and advancements in information and communication technology (ICT) to accelerate economic growth, narrow social and geographic gaps, and promote an inclusive and efficient government.[72]

3.1.5 Cybersecurity strategy

Germany

The cybersecurity strategy for Germany was developed by the BMI in 2021[73] and defines the strategic framework for the federal government's actions in the area of cybersecurity for the next five years. Several upcoming cyber threats were identified as relevant scenarios to derive the necessary implementation goals. Consistent with the findings in Section 2.3, these scenarios include new attack vectors resulting from the increased connectivity of devices to the Internet, supply chain attacks, ransomware attacks, DoS (ransom) attacks as well as APTs initiated or supported by enemy states. Thus, the relevant fields of action of the cybersecurity strategy include:

1. *Safe and self-determined action in a digitalised environment* to strengthen the cyber competence of citizens and the consumer protection;
2. *Joint mission of the state and economy* to strengthen the cybersecurity of the economy, with a greater focus on critical infrastructure, especially regarding small and medium-sized companies;
3. *Powerful and sustainable state-wide cybersecurity architecture* to improve cooperation between national authorities; and
4. *Active positioning of Germany in European and international cybersecurity policy* to improve engagement in the EU and NATO.

Additionally, the BMI introduced a cybersecurity agenda in 2022[74] to define more specific goals and actions for improvement of cybersecurity in Germany up to the year 2025. The relevant agenda points and actions include:

1. Strengthen the skills of national authorities, especially BfV and BKA (e.g., to cope with cyber-attacks from foreign states);
2. Protect the civilian infrastructure against cyber-attacks by establishing BSI information sharing portals and initialising a civilian cyber defence centre;
3. Extend the confirmation testing capabilities of the BSI regarding manufacturers for critical infrastructures (e.g., in the energy sector); and
4. Improve the cyber resilience of critical infrastructures by providing financial support for cyber resilience investments in small and medium-sized companies, by establishing awareness and cyber resilience projects, by integrating supply chain security into the regulation of critical infrastructures and by establishing sector-specific CERTs that have strong links to the BSI situational awareness centre.

[72] Ministry for Social Equality (2017)
[73] Bundesministerium des Innern und für Heimat (2021)
[74] Bundesministerium des Innern und für Heimat (2022)

Israel

Addressing cyber threats is among the top national political and security priorities for both Israel's military and civilian sectors. In 2017, the Israel National Cyber Directorate (INCD) published a whitepaper[75] formulating a plan to improve Israel's cyber robustness, systemic resilience and civilian cyber defence. This is the first comprehensive official national cybersecurity strategy since Ben Gurion's (first Prime Minister of Israel) declaration of strategic principles from 1953[76]. These doctrinal principles include deterrence of enemies, decisive victory, early warning and alliances. The relevant parts of the cybersecurity strategy from 2017 include:

5. *Civilian cyber defence* as a three-layer approach for cyber robustness, systemic cyber resilience and civilian cyber defence;
6. *Capacity building* for the foundation of cyber operations by educational and industrial efforts from state-owned industries, commercial research and development as well as academic research; and
7. *Mandating the INCD* with the supervision and implementation of cyber operations.

The first layer of civilian cyber defence fosters an aggregated cyber robustness against daily threats by promoting security efforts in the private sector. Here, the INCD sets mandatory standards for essential sectors and critical infrastructures. The second layer cultivates a systemic cyber resilience by improving cooperation between national and international authorities. Also, incident response and early warning capabilities will be improved by way of intelligence gathering and the sharing of sector-relevant information. The Israeli Cyber Emergency Response Team (CERT-IL) coordinates the system cyber resilience efforts. The third layer enhances the civilian national cyber defence to mitigate the most severe cyber threats to national security. In 2024, the INCD started to update the national cyber defence strategy by formulating a vision for a secure and trustworthy digital space and strengthening the national cyber resilience in the different sectors.[77]

[75] STATE OF ISRAEL PRIME MINISTER'S OFFICE (2017)
[76] Freilich (2018)
[77] Israel National Cyber Directorate (2023)

3.2 Summary of key facts

Based on the findings from the previous section, Table 1 (see below) provides a short comparison of the underlying infrastructure and regulations in Germany and Israel.

Table 1: Comparison of electrical infrastructure in Israel and Germany

	Israel[78, 79]	Germany[80]
Electrical energy		
Annual production	75 TWh	513 TWh
Share of RES	11.3%	52.9%
Transmission system		
Operators	1	4
Ownership	Private	Public, private
Voltage levels (line length)	400 kV (806 km) 115/161 kV (5,065 km)	220–380 kV (37,700 km)
Distribution grid		
Operators	1	866
Ownership	Public, private	Public, private
High-voltage (line length)	-	110 kV (95,000 km)
Medium-voltage (line length)	12.6, 22, 33 kV (30,113 km)	3–30 kV (530,000 km)
Low-voltage (line length)	0.4 kV (40,955 km)	< 1 kV (1,250,000 km)
Regulation and markets		
Regulatory bodies		
Governmental	MoE	BMWK, BMI State governments: telecommunication networks
Institutional	INCD Public Utility Authority for Electricity (PUA)	BSI ENTSO-E (EU body, international institution) BNetzA
Grid stability	PUA	ENTSO-E (EU body, international institution) BNetzA: power quality requirements
Grid connection	IEC	DSOs: technical requirements for units connecting to grid BDEW, VDN: provide template for requirements

[78] Gutglik et al. (2023)
[79] Weinstock und Elran (2017)
[80] BDEW Bundesverband der Energie- und Wasserwirtschaft (2023a)

4 State of digitalisation in Germany and Israel

Digital technologies are essential for the future design of the electrical energy sector. They enable the integration of the renewable energy sources that are needed to decarbonise the energy system, all while maintaining efficiency, reliability and a security of supply. The major transformation taking place due to renewable sources is accompanied by system flexibilities such as electricity storage systems, BEVs and demand response mechanisms. This shift is complemented by liberalised energy markets that facilitate trading and by the widespread deployment of smart meters that can facilitate real-time monitoring of electricity usage and power quality. Additionally, the convergence of IT and OT introduces innovative technologies like cloud services, virtualisation and wireless networks, further optimising energy management and efficiency.

From Section 3.1, the digital strategy in the German energy sector focuses on intelligent metering systems and data spaces or platforms. The energy transition (see Section 3.1.2) leads to a highly decentralised energy system with a high share of wind and solar production. The resulting large number of local energy providers and renewable energy installations is mainly owned by municipalities, cooperatives and private companies. Israel, known as a start-up nation, follows a digital programme to leverage advancements from digital technologies and maintain its position as a leading technological innovator. The Israeli energy infrastructure is highly centralised, albeit with an increasing share of private ownership (newly built as well as purchased from the IEC[81]). Energy production includes conventional and renewable sources sharing few if any connections to neighbouring countries, making Israel somewhat of an energy island (initiatives like the EuroAsia Interconnector aim to link Israel's grid with those of Cyprus and Greece, enhancing regional energy integration[82]). This chapter analyses the current state of digitalisation in the energy sectors of Germany and Israel and presents:

- a description of energy market roles and processes as well as an analysis of implemented smart meter systems in Section 4.1;
- an analysis of the capacities installed and electrical energy produced by RES as well as the energy consumption in Section 4.2; and
- a description of the transmission and distribution systems including communication technologies and expansion measures in Section 4.3.

The research is based on publicly available regulatory documents, standards, reports, guidelines and studies. Additional workshops were held with different representatives from the energy and cybersecurity industry from both countries to sharpen and prioritise the research analysis. For the comparative analysis in Chapter 6, a list of indicators is derived in Section 4.4 to assess the state of digitalisation in both countries.

4.1 Energy market and metering

Market participants and their growing interdependencies highlight the increasing complexity of energy markets, which require advanced digital platforms for seamless coordination and efficient management. Innovative business models (e.g., P2P trading, dynamic tariffs) rely heavily on digital tools for implementation and optimisation, reflecting the transformative potential of digitalisation (see Table 2). Market data exchange and the availability of digital platforms demonstrate the level of integration in market operations, with advanced metering infrastructure, real-time data sharing and easy access to metering data enabling better energy management and decision-making for all stakeholders.

[81] Wrobel (2023)

[82] Mitchell (2021)

Table 2: Drivers of digitalisation in the energy market and metering

Factors driving digitalisation	Solutions identified
• Markets: roles, interactions and coordination • Business models, tariffs, billing and settlement (such as peer-to-peer energy trading and demand response programmes)	• Data exchange • Smart meters (requirements and deployment) • Value-added services

4.1.1 Germany

The liberalisation and unbundling of the energy sector have created a vast number of market roles and stakeholders. Facilitating efficient and standardised interactions between market participants is crucial for unlocking the benefits of a competitive electricity sector. The regulatory framework, governed by laws such as the EnWG, MsbG, NA-BEG 2.0 and StromNVZ, supports these processes and ensures effective data exchange. [83, 84]

The energy market model

The German approach defines market roles for key participants such as TSOs and DSOs, plant operators, metering point operators or the roughly 1,350 suppliers. Balancing coordinators manage financial settlement under the four TSOs, whilst balancing group managers oversee power across approximately 10,500 groups, each involving a variety of the 1,500 market participants. All this is supported by software and data providers that facilitate information exchange throughout the various technical communication processes.

Regulated market communication in the energy sector is facilitated by established processes, including, but not limited to: business operations for retail and contracts (e.g., supplier changes), market rules for balancing group invoicing and data exchange (e.g., metering data), and procedures for determining over- and under-supply, requiring coordination between suppliers and system operators, and reporting to the BNetzA. Most market processes are overseen by the BNetzA in accordance with the EnWG and MsbG to ensure transparency, compliance and reliable operations.[85, 86].

Business models

Germany's electrical supply sector is experiencing a shift towards innovative business models and new tariff structures to support the energy transition. Dynamic pricing models, such as time-of-use and real-time tariffs, are gaining popularity, incentivising consumers to shift electricity usage to periods of lower demand or higher renewable energy availability. Subscription-based models and flat-rate pricing for renewable energy packages are also emerging, offering predictable costs and promoting green energy adoption. Additionally, novel peer-to-peer energy trading platforms within a supplier eco-system enable prosumers to sell surplus electricity directly, fostering local energy communities and decentralised grid management.

Data exchange and data platforms

The growing digitalisation of the energy sector has led to an increase in digital processes and business models requiring secure and efficient data exchange to meet regulatory standards. To address this, the BSI has introduced cybersecurity measures, including certified private signature keys, encryption technologies and a smart metering public key infrastructure, though current encrypted e-mail data transfers remain inefficient and web service automation (e.g., using AS2 or AS4 standards) is not yet cost-effective.[87, 88, 89]

[83] Bundesnetzagentur (2025a)
[84] NABEG (2025)
[85] Bundesnetzagentur (2025b)
[86] Bundesnetzagentur (2025c)
[87] Knüsel and Richard (2022)
[88] Böswetter and Richard (2021)
[89] Böswetter et al. (2021)

Data exchange between system operators improves efficiency and security of supply by integrating market and grid data[90]. Standardisation efforts like the Common Information Model (CIM) offer a framework for innovative service models like Energy as a Service (EaaS), virtual power plants (VPPs) and demand forecasting.[91]

Unlocking the full potential of the liberalised energy market will require data spaces and platforms as a basis for new market processes and business models in the energy market. Connect+[92] represents a first attempt to establish a platform to share redispatch data between system operators. The GAIA-X initiative[93] is seen as a possible future data platform across different domains and sectors.

Smart metering and deployment

Germany's Smart Meter Gateway (SMGW) is a key component in digitalising the energy sector. It forms a type of programmable data concentrator and has the potential to securely connect versatile sensors and actuators (digital meters, generator control units) with grid operators, energy suppliers and service providers to enable use cases such as real-time energy data, demand response, automated billing and the control of small generators and power electronics on a vast scale.

Developed under BSI regulations with a trusted platform module (TPM) and incorporating security and privacy by design principles, the SMGW offers solid data protection and cybersecurity. Initiatives like the Future Energy Lab[94] are pioneering digital identities for device authentication in highly automated energy systems.

The deployment of smart meters is firmly anchored in the German digital strategy. Phased installations regulated under the EEG and MsbG require 95 per cent of consumers above 6,000 kWh per year and producers above 7 kW to switch to smart meters by 2032. Consumers below 6,000 kWh per year and small producers are being transitioned over to digital meters. While connection to the ICT network is not required, it is expected to be incentivised by new business models and services.[95]

Communication technologies

The communication infrastructure for grid management relies on fibre optic, copper and coaxial cables, with 450 MHz technology enhancing reliability for remote and underground smart meter installations. In Germany, 71 per cent of smart meters use LTE, 14 per cent power line communication (PLC) and 4 per cent use DSL. While real-time monitoring is advanced at high-voltage levels, it faces digitalisation-related challenges in rural low-voltage networks.[96, 97]

Value-added services

The goal of fostering value-added services through the SMGW infrastructure remains elusive, having been throttled by complex requirements and lengthy certification processes. Current business models operate predominantly outside of the SMGW infrastructure. Cohesive regulation and more ambitious targets (such as the requirement for suppliers to offer dynamic tariffs) are designed to drive the adoption of SMGW as the standard for (potentially critical) data-driven energy services.

[90] Shaping Europe's digital future (2025b)
[91] ENTSO-E (2025b)
[92] Amprion (2025)
[93] DKE (2022)
[94] dena Future Energy Lab (2025)
[95] Böswetter et al. (2021)
[96] Bundesnetzagentur (2023)
[97] KPMG (2025)

4.1.2 Israel

The digitalisation of Israel's energy market is underpinned by comprehensive policy frameworks, significant investments in smart technologies and a strong focus on regulatory compliance. Israel's approach to energy market liberalisation has significantly reshaped the sector, creating a competitive environment where private companies play an increasingly prominent role.

Israel's evolving energy market model

From the end-customer's point of view, a main effect of the market reform is the ability to choose a supplier from a growing number of private companies. While private energy producers have been increasingly supplying the IEC for several years,[98] commercial consumers and households have just recently been given access to a supplier market. In 2023, the MoE, under the guidance of the PUA, implemented significant reforms to enhance competition and allow non-discriminatory integration of RESs[99]: Key regulated mechanisms include:

- *Market participation of RES facilities*: In 2022, the PUA made a pivotal decision to allow renewable energy facilities to participate in the electricity market at the transmission level. This move enabled independent power producers to sell electricity directly to large end consumers, promoting the adoption of green energy[100].
- *Contracts with private suppliers*: By early 2024, the PUA facilitated contracts between private suppliers and end consumers, allowing households to choose their electricity providers. This initiative aimed to reduce electricity bills by an estimated five to 20 per cent and marked a significant shift from the previous monopoly held by the state-owned IEC[101].

These reforms have empowered Israeli consumers to select from various electricity suppliers, fostering competition and potentially leading to cost savings. The integration of diverse vendors and renewable energy sources introduces cybersecurity challenges but enhances grid resilience by reducing single points of failure and stabilising the system, while also aligning with global sustainability goals and improving energy security.[102]

This diversification has been facilitated by government incentives and regulatory reforms designed to attract private investment, particularly in renewable energy projects.

Deployment of smart meters

The rollout of smart meters is central to Israel's digital transformation in the energy sector. The PUA has implemented a regulatory framework to accelerate their deployment, emphasising the importance of these devices for real-time monitoring and efficient grid management. By the end of 2021, Israel's installed base of smart meters had grown significantly, spurred by a focus on equipping them with remote read-out capabilities. These smart meters not only collect detailed energy usage data but also enable two-way communication between consumers and utility providers, enhancing grid reliability and operational efficiency[103]. This progress was further bolstered in 2022 when the IEC launched an ambitious plan to install one million smart meters over five years, targeting 200,000 installations annually[104].

The introduction of smart meters has empowered consumers by providing real-time insights into their energy consumption, encouraging energy-saving behaviour and enhancing overall market efficiency. These measures collectively support the development of a more dynamic, consumer-driven energy landscape in Israel.

The IEC's initiative aims to achieve near-total coverage of consumers in the coming years, enabling widespread smart meter adoption to support dynamic energy pricing and advanced energy management services. Data granularity is a key focus in Israel's energy market, as high-resolution energy consumption data is essential for grid analytics and optimising energy distribution. Regulatory bodies in Israel are developing guidelines for data sampling rates to ensure robust data collection. While detailed standards are still under development, the overarching goal is to maximise the utility of energy data while safeguarding consumer privacy and data security.

---

[98] Technology (2023)
[99] Gov IL (2024c)
[100] Global Legal Group (2025)
[101] Enerdata (2024)
[102] ScienceDaily (2025)
[103] IoT M2M Council (2023)
[104] Globes (2022)

Communication technologies

Communication technologies are essential for supporting the digitalisation of Israel's energy market. The increased deployment of advanced networks, including fibre optics and wireless communication systems, ensures that data collected from smart meters is transmitted securely and efficiently[105]. These systems enable seamless integration of digital business models, such as automated billing and demand-side management, which rely on accurate and timely energy data[106]. The use of secure communication protocols is prioritised, with robust cybersecurity measures being implemented to protect sensitive information from potential threats[107]. The use of secure communication protocols is prioritised in Israel's energy sector, with robust cybersecurity measures being implemented to protect sensitive information from potential threats. This digital transformation is supported by comprehensive policy frameworks, significant investments in smart technologies and a strong focus on regulatory compliance[108].

4.2 Distributed energy production: integration of renewables

Both Israel's and Germany's energy systems are undergoing significant transformations, driven by the integration of renewable energy sources through distributed energy resources (DERs), which are crucial in meeting national energy transition goals (see Table 3)[109].

As the share of renewable energy increases, the importance of digitalization also grows — enabling more effective monitoring, control, and system integration. While both countries are pursuing this transition, the current share of renewables differs significantly between Germany and Israel. This shift is assessed through a set of KPIs that highlight both the need for digital technologies and the current level of digitization in the context of distributed energy production.

Table 3: Digitalisation drivers for distributed energy production

Factors driving digitalisation	Solutions identified
• Increasing share of DERs • Grid stability • Grid connection processes	• Virtual power plants • Distributed energy resource management systems (DERMS) • Digital planning tools • Announcements and investments

4.2.1 Germany

Renewable energy sources have long been a staple of the German energy system with the aim of achieving a transition to net zero electricity generation by 2040. The combined efforts in regulatory adjustments, infrastructure investments and technological advancements are shaping a resilient energy grid that aligns with Germany's renewable energy targets. Continued support for DERs, through reduced costs, regulatory facilitation and smart grid developments, is essential for realising a sustainable, flexible energy future.

[105] Central (2024)
[106] Weizenblut (2024)
[107] Science|Business (2025)
[108] Ganot (2024)
[109] Aggregators (2019)

Installed capacity and energy production

The installed capacity for DERs has risen substantially, primarily due to favourable policies, regulatory frameworks and technological advancements promoting renewable sources like wind and solar. This expansion of decentralised generation highlights Germany's dedication to diversifying energy sources and lessening its dependence on fossil fuels. However, regional variations exist: Rural areas with greater renewable potential often face limitations due to grid constraints, requiring ongoing infrastructure improvements to optimise DER integration.[110]. By 2022, the total renewable energy capacity reached 150.4 GW, with onshore wind accounting for 59.3 GW and solar energy for 73.97 GW. Projections under the EEG show ambitious targets, with solar energy capacity expected to rise to 215 GW and onshore wind to 115 GW by 2030.[111], [112], [113], [114], [115], [116], [117]

Interconnection time

The interconnection timeline, defined as the period from regulatory approval to physical grid connection, varies in Germany depending on the type of consumer or producer, with shorter timelines for end consumers, moderate timelines for small to medium-sized renewable installations and longer timelines for large power plants due to complex approval processes and potential grid expansions. Delays persist, especially in rural areas with less developed grid infrastructure. In more populated areas, however, interconnection timelines have improved significantly as streamlined regulatory processes reduce wait times[118]. The introduction of digital solutions aims to alleviate delays by implementing standardised protocols and ensuring real-time coordination between DERs and DSOs. These advancements in regulatory and administrative processes will play a crucial role in accelerating DER contributions to grid stability and renewable targets, particularly during high-demand periods[119].

Virtual power plants and demand response

Virtual power plants (VPPs) in Germany are networks that connect decentralised energy producers, flexible consumers and storage systems. One of Europe's largest VPPs, operated by Next Kraftwerke, has over 10,000 MWs of interconnected capacity, mostly from solar power. These systems use smart controls to manage electricity supply and demand flexibly, functioning like a traditional central power plant. Statkraft also operates a major VPP in Germany, linking more than 1,600 wind and solar parks with a total capacity of around 12,000 MW.

The demand response participation among DERs is steadily rising, driven by market incentives and advancements in grid technology. Demand response programmes allow DERs to adjust output in response to real-time grid demands, enhancing grid flexibility and supporting supply-demand balance during peak periods or low renewable output[120]. With more DERs engaging in demand response, Germany is better equipped to handle the variability of renewable energy, thus fostering a resilient grid system. Technological innovations, including virtual power plants, are facilitating greater participation from DERs, helping Germany to align energy generation with consumption patterns and further reduce reliance on fossil-based generation[121].

[110] Umweltbundesamt (2025)
[111] Statista (2025d)
[112] Clean Energy Wire (2022)
[113] Bundesnetzagentur (2023)
[114] Statista (2025a)
[115] International Renewable Energy Agency (2015)
[116] IEA (2025b)
[117] Website of the Federal Government | Bundesregierung (2025)
[118] Bundesnetzagentur (2025d)
[119] VDE (2025)
[120] Sonnen (2025)
[121] E3P (2025)

4.2.2 Israel

Israel's transition to distributed energy production is a cornerstone of its energy strategy, aimed at reducing fossil fuel dependency and achieving ambitious renewable energy targets. In 2019, Israel raised its renewable energy targets to 10 per cent by 2020, 20 per cent by 2025 and 30 per cent by 2030, requiring an estimated $22 billion investment and significant efforts in the area of infrastructure, technology and policy reforms to achieve these goals.[122, 123]

Installed capacities and energy production

By the end of 2021, the country had installed approximately 3,656 MW of renewable energy capacity, representing 9.4 per cent of its total energy consumption[124]. Solar energy plays a dominant role, supported by Israel's favourable climate and many hours of sunshine, with solar installations comprising the majority of renewable capacity. By 2023, renewable energy accounted for 12 per cent of Israel's electricity generation. To bolster progress in this area, approximately 2.6 GW of storage facilities are planned, with around one third connected to the ultra-high-voltage grid and managed by the system operator. Electricity demand is expected to grow by 3.1 per cent by 2030 and 3.7 per cent between 2030 and 2040[125].

Virtual power plants (VPP)

Virtual power plants (VPPs) are an emerging sector in Israel, with companies offering software solutions to manage portfolios of dispersed generation units. VPPs unlock their full potential, especially when combining larger amounts of solar modules and storage capacities, to enhance grid flexibility and optimise energy distribution. These systems can aggregate and balance decentralised energy resources, improving efficiency and reliability.

Distributed energy resource management systems (DERMS)

The necessity for DERMS in Israel is underscored by the expected growth of its distributed energy sector and the increasing complexity of managing renewable energy assets. DERMS platforms enable integrating distributed generation, storage and energy trading by coordination and optimising the diverse energy resources. This technology not only enhances grid resilience but also maximises profitability for stakeholders.[126]

The integration of renewable energy into Israel's national grid has necessitated advanced grid management solutions due to the inherent variability of sources like solar and wind energy, which are subject to weather-related fluctuations. To maintain grid stability and balance supply and demand, the PUA has invested in energy storage technologies, including large-scale battery systems and pumped hydro storage. Notably, planning authorities have approved a blueprint for an 800MW/3,200MWh energy storage park that includes diverse energy storage technologies[127]. Additionally, real-time monitoring and automation have been introduced to optimise grid performance and ensure reliable energy distribution, even during peak demand or periods of low renewable generation. The IEC has extended its partnership with Prisma Photonics to monitor over 1,000 km of the national grid, enhancing fault detection and response capabilities[128].

Interconnection timeline

One of the key metrics for assessing the efficiency of distributed energy production is the interconnection timeline, which refers to how long it takes to connect new renewable energy facilities to the grid. Historically, long approval and connection processes have posed barriers to the rapid deployment of renewable energy projects[129]. Recognising this challenge, PUA has implemented reforms that have streamlined these procedures, significantly reducing the time needed to bring new facilities online. In areas with high solar energy potential, interconnection timelines have been shortened to just a few months, supported by digital solutions and simplified regulatory frameworks[130]. These measures have improved the integration of renewable energy sources into the national grid, fostering Israel's shift towards a more sustainable energy system.

---

[122] Shakhak (2023)
[123] Surkes (2020a)
[124] Ganot (2022)
[125] Mizrahi et al. (2024)
[126] Desk (2024)
[127] Energy Storage Journal (2025)
[128] T&D World (2024)
[129] OECD (2025)
[130] Proaktor et al. (2023)

4.3 Transmission and distribution system

Transmission and distribution grids are vital to energy infrastructure, and their role is increasingly crucial with the integration of intermittent renewable energy sources like solar and wind. In order to maintain stability while minimising the need for expensive, advanced grid management solutions, such as real-time monitoring, smart grids and energy storage, are being implemented to optimise energy flows and ensure reliable distribution (see Table 4).

Table 4: Drivers of digitalisation for grid operation

Factors driving digitalisation	Solutions identified
• Increasingly complex grid operations • Congestion and need for new power lines or reinforcement	• Advanced distribution management systems (ADMS) • Increasing observability of grid state

4.3.1 Germany

Germany's electricity grid is undergoing a significant transformation to support its energy transition. Continued investments in infrastructure, technology and renewable integration remain crucial for enhancing grid efficiency and reliability, ensuring it meets future demands while advancing the nation's sustainability goals.

Grid expansion and development

Germany's electricity network is a complex and evolving system, balancing the integration of renewable energy sources with the demands of a robust infrastructure. Managed by four TSOs and 866 DSOs, the grid comprises 36,300 km of transmission lines and approximately 2.2 million km of distribution circuits as of 2022, supporting 52 million market locations. Renewable energy sources contributed 44-45 per cent of gross electricity consumption in 2022, including 22 per cent from wind power and 11 per cent from photovoltaics. However, integrating these intermittent energy sources presents challenges, requiring advanced grid management solutions such as real-time monitoring, HVDC voltage stabilisation, automation and predictive maintenance to maintain stability. Investments in grid infrastructure totalled €13.12 billion in 2022, with €8.84 billion allocated by DSOs (an 18 per cent increase) and €4.28 billion by TSOs (a 19 per cent decrease).

The grid stability index measures the system's ability to maintain stable frequency and voltage levels amid growing renewable integration[131]. Metrics include frequency regulation, voltage control and grid disturbance rates. German TSOs maintained stability in 2022 through actions like real-time monitoring, advanced digital technologies and HVDC systems, enabling the integration of 531.7 TWh of renewable energy, including 20.4 per cent from wind power[132].

Germany's grid expansion is guided by the Federal Requirement Plan Act (BBPlG) and Energy Line Expansion Act (EnLAG), covering 119 projects totalling 14,054 km by the end of 2022. EnLAG accounted for 1,821 km, with 1,356 km completed, while BBPlG projects spanned 12,233 km, including 1,103 km completed. Future investments of €42 billion by 2032 are planned to strengthen, optimise or replace 93,136 km of grid infrastructure, with 32 per cent of projects under construction. Peak demand in 2022 reached 78.83 GW, illustrating the grid's capacity to accommodate demand, including transmission losses.

[131] Vega Penagos et al. (2024)

[132] Kumar and De (2024)

Despite these measures, challenges such as grid congestion led to the curtailment of 8 TWh of renewable energy in 2022, an increase from 5.8 TWh in 2021[133]. Redispatch costs rose to €2.69 billion, underscoring the need for enhanced grid integration and expanded infrastructure to reduce future curtailments and economic impacts. Regional energy mixes across Germany's federal states reflect significant renewable contributions, particularly from wind and solar, with variations in reliance on non-renewable sources like brown coal, black coal and natural gas.[134, 135, 136]

To address these challenges, Germany continues to prioritise investments in grid modernisation, deploying advanced technologies and fostering the integration of distributed generators such as DERs as part of its energy transition strategy.

Technology and grid modernisation

The implementation of intelligent substations, including digital and secondary substations, is driving advancements in grid transparency and efficiency as part of Germany's energy transition. These substations utilise intelligent electronic devices (IEDs) to enable real-time monitoring and control of grid assets, offering advanced capabilities such as automated fault detection, self-healing mechanisms and integration with SCADA systems. By automating data acquisition and decision-making processes, they significantly reduce operational costs and improve reliability. A notable example is the high-voltage substation in Burladingen, Germany, the world's first eco-efficient facility operated without SF6 gas, fully digitalised with advanced equipment connectivity and intelligence. This eco-friendly, state-of-the-art substation demonstrates a significant step towards future-orientated, digitally enabled substations. Germany has an estimated 600,000 secondary substations serving as nodes between medium- and low-voltage networks. While the exact number of substations already upgraded to digital or intelligent systems is not publicly available, grid operators are making substantial investments in modernisation. For example, Westnetz GmbH, a subsidiary of Westenergie AG, commissioned around 1,000 digital secondary substations in 2024. Similarly, companies like MITNETZ STROM aim to digitalise or equip up to 25 per cent of their substations with advanced measurement technology by 2026. E.ON has also committed to the digitalisation of approximately 28,000 secondary substations by 2026, connecting them to the 450 MHz frequency network. In 2024 alone, E.ON plans to install about 5,000 new digital secondary substations equipped with fail-safe 450 MHz communication technology. These efforts highlight the growing integration of environmentally friendly practices and cutting-edge technology, showcasing a clear trend towards modernising the power grid to enhance supply security and meet the demands of the energy transition.

4.3.2 Israel

Grid expansion and development

The transmission and distribution system in Israel is undergoing significant upgrades to accommodate the rise of renewable energy. Managed primarily by the IEC, the T&D system has seen investments totalling approximately NIS 3 billion (EUR 750 million) in 2021 alone[137], directed towards expanding the high-voltage transmission network and integrating smart grid technologies that improve efficiency and reliability. In addition, IEC has expanded its collaboration with Electrical Grid Monitoring™ (EGM) Inc. to enhance distribution and transmission solutions[138]. This partnership aims to provide advanced grid management systems, including pilot installations in southern Israel's transmission grid, managed by Noga. The variability of solar energy, for example, can cause frequency and voltage fluctuations that impact the stability of the grid. To address this, the IEC has implemented advanced grid management solutions, including real-time monitoring and automation. These technologies enable grid operators to quickly respond to changes in energy supply and demand, ensuring a stable and continuous power supply[139].

High-voltage transmission lines are essential for transporting electricity over long distances, especially from remote solar farms to urban centres. The IEC has prioritised the development of these lines, with a particular focus on regions that have high renewable energy potential. For instance, energy generated from large-scale solar farms is often transmitted via newly constructed high-voltage lines, minimising transmission losses and improving overall grid efficiency[140]. Medium-voltage networks are also being expanded to ensure that energy can be efficiently distributed to residential and industrial consumers[141].

---

[133] Federal Statistical Office (2023)
[134] Statista (2025c)
[135] Statista (2025b)
[136] eG (2025)
[137] Israel Electric Corp. (2021)
[138] Yehuda (2023)
[139] Israel Electric Corp. (2023)
[140] Israel Electric Corp. (2018)
[141] kgi-admin (2023)

Technology and grid modernisation

Energy transmission losses remain a concern, especially in the lower voltage distribution networks. Efforts to reduce these losses include upgrading infrastructure and implementing more efficient transmission technologies. According to the latest data, transmission losses have been minimised to ensure that energy is delivered efficiently, though the system still faces challenges in managing peak loads and ensuring reliable energy distribution across all regions. The IEC is actively working to address these issues by deploying smart grid technologies that optimise energy flow and reduce losses[142].

Another critical issue is energy curtailment. During peak periods of renewable energy generation, the grid sometimes cannot accommodate the excess energy, leading to curtailment. To mitigate this, the Electricity Authority has been investing in energy storage solutions, such as large-scale batteries and pumped hydro storage, to store excess energy for later use. These investments are crucial for ensuring that renewable energy can be fully utilized and for enhancing grid flexibility[143].

Communication infrastructure is also being enhanced to support the digitalisation of the T&D system. Secure and efficient communication networks are essential for real-time data exchange between energy producers, grid operators and consumers. The implementation of advanced communication technologies, such as fibre optics and wireless networks, has improved the reliability and speed of data transmission. This is particularly important for managing a smart grid, where timely and accurate information is crucial for optimising energy distribution and responding to grid disturbances[144]. Figure 8 illustrates investment trends for 'transport' and 'distribution' from 2008 to 2021. The transport line (light blue) shows steady growth, while the division line (dark blue) fluctuates but rises overall. By 2021, transport investments surpass those in division.

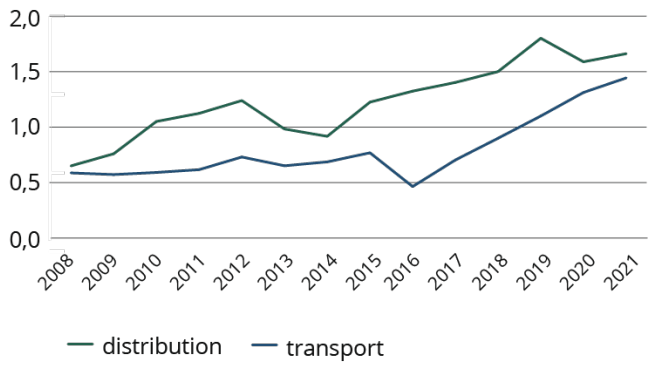


Figure 8: Electricity company investments in opening up the electricity network in billions of shekels[145]

Efforts to modernise the transmission and distribution system are part of a broader strategy to create a more resilient and efficient energy infrastructure. These initiatives are critical for meeting Israel's renewable energy targets and ensuring that the grid can handle the increasing complexity of a decentralised energy system. However, continued investment and innovation will be required to fully integrate renewable energy sources and to prepare the grid for future energy demands.

4.4 Digitalisation indicators

Based on the findings from Sections 4.1, 4.2 and 4.3, a comprehensive set of digitalisation indicators and metrics has been derived which are presented in to assess and compare the state of digitalisation in Germany and Israel. These indicators include smart meters, which offer vast potential for utilities and grid operators to plan and operate highly efficient and reliable infrastructures. The penetration rate of digital meters with remote read-out capabilities is a key metric in this context. Additionally, the granularity (sample rate) of measurements, regulated by national regulatory bodies or required by utility companies, serves as an important indicator. Higher sample rates allow for more in-depth analysis, supporting advanced digital business models and services offered to consumers. National policies regarding smart meter deployment further reflect the strategic approach towards grid digitalisation.

[142] POWERGRID International (2025)
[143] POLITICO (2024)
[144] Nhede (2017)
[145] Shakhak (2023)

The deployment of communication networks for smart meters demonstrates the grid's readiness to support digital devices and functionalities, while the total number of smart meters deployed underscores the transition to automated, digitalised energy monitoring. The granularity of smart meter data enhances the ability to perform detailed real-time energy analysis, facilitating advanced analytics and demand-side management. Expanding smart meter coverage reflects the commitment to ensuring digital inclusivity among consumers, while national policies further shape the pace of deployment.

The installed capacity of RESs and the efficiency of these systems, measured through metrics such as capacity factor and actual energy output, provide insights into the substitution of fossil fuels and the effectiveness of policies fostering RES penetration. Monitoring the output of distributed energy resources (DERs) compared to their potential maximum output relies on real-time digital tools to optimise performance and reliability. Accurate tracking of renewable energy production as well as total energy consumption by industry and households is facilitated by digitalised data collection systems, which also enable demand response and energy efficiency initiatives.

The capacity to integrate new RESs into the grid efficiently is reflected by the time required to respond to connection requests and the costs associated with regulatory compliance and grid interconnection. Lower connection times and costs highlight the effectiveness of digitalised workflows and infrastructure. Metrics such as the percentage of curtailed energy from DERs and the extent of real-time monitoring systems illustrate the ability of grid operators to optimise energy usage, maintain grid stability and minimise losses.

The use of advanced and redundant communication technologies underscores the importance of robust communication infrastructure, which supports data integrity, system resilience and operational efficiency. Together, these indicators provide a comprehensive framework for evaluating the progress of digitalisation in power grids, offering valuable insights into system efficiency, sustainability and market competitiveness. By integrating these metrics, the study highlights achievements and identifies opportunities for further advancements in digitalised energy systems. Table 5 lists the defined digitalisation indicators and chosen metrics for this study.

Table 5: Overview of defined digitalisation indicators

Indicator	Basis for assessment (metric)
Energy market and metering	
Market participants	• Amount of market roles and degree of interdependencies
Market business models	• Use of business models and degree of added values for companies
Market data exchange and platforms	• Kind of exchanged market data • Availability of access to metering data • Availability of communication networks for smart meters
Percentage of smart meters	• Percentage of smart meters in relation to total installations with and without remote reading
Smart meter data	• Sampling rate of measurements and parameters
Coverage of consumers with smart meters	• Actual coverage and planned (time horizon) coverage
Distributed energy producers	
Installed capacity of RESs and capacity factor	• Total capacity of actual installed conventional and renewable power plants • Planned capacities of conventional and renewable power plants • Output of DERs compared to their potential maximum output
Energy production by RESs	• Total amount of conventional and renewable energy production
Interconnection timeline	• Average time required for DERs to connect to the grid after approval
Installed capacity of RESs and capacity factor	• Total capacity of actual installed conventional and renewable power plants • Planned capacities of conventional and renewable power plants • Output of DERs compared to their potential maximum output
Transmission and distribution system	
System size	• Circuit length at high-, medium- and low-voltage levels
Energy curtailment rate	• Percentage of energy generated by DERs that is curtailed or not used due to grid constraints
State of digitalised supervision	• Extent of used real-time monitoring and control systems as well as automation processes
Communication infrastructure	• Use of advanced and redundant communication technologies

5 State of cybersecurity in Germany and Israel

Cybersecurity in the electrical energy sector is crucial to ensure an uninterrupted power supply and to protect the infrastructure from increasing cyber threats. As referenced in Section 2.3, this especially requires cybersecurity measures for OT systems taking into account legacy or proprietary technology. Effective cybersecurity strategies are essential to protect OT systems from emerging threats like ransomware-as-a-service or malware infections, safeguarding not only the energy sector but also other critical infrastructures that depend on it.

As referenced Section 3.1, the German energy infrastructure is highly decentralised to accommodate the ongoing integration of renewable energy sources and is therefore characterised by many municipalities, cooperatives and private companies. This leads to a high number of possible entry points for cyber threat actors at the transmission and distribution level of the power system. The German cybersecurity agenda focuses on the protection of critical infrastructures, especially financial support for SMEs and ensuring supply chain security, including manufacturers and providers. The Israeli energy infrastructure is highly centralised and independent from neighbouring countries ('desert island'). Especially since Operation Iron Swords, Israel is facing a significant number of physical and cyber-based attacks. Thus, the handling of cyber threats has utmost national priority and is based on a proactive cyber defence strategy with a strong cooperation between the military and civilian cyber space as well as major investments to engage civilian cyber capabilities.

This chapter analyses the current state of cybersecurity in the energy sectors of Germany and Israel and presents:

- a review of the regulating authorities, non-government institutions and contact points (e.g., for incident response plans) as well as the presence of information sharing platforms (e.g., for advisories or vulnerabilities) in Section 5.1; and
- an analysis of the relevant cyber threats, including systemic vulnerabilities and their impact on the energy sector in Section 5.2.

The research is based on publicly available regulatory documents, standards, reports, guidelines and studies. Additional workshops were held with different representatives from the energy and cybersecurity industry from both countries to sharpen and prioritise the research analysis. For the comparative analysis in Chapter 6, a list of indicators is presented in Section 5.3 to assess the state of cybersecurity in both countries.

5.1 National authorities and contact points

5.1.1 Germany

Cybersecurity is becoming more and more important for national security and is accompanied by increased digitalisation and networking in Germany. In general, the BMI is responsible for domestic cyber policy, appoints a federal commissioner for information technology and supervises the BSI for the operational implementation of the national cybersecurity strategy (also see Section 3.1). The cyber defence is based at the Federal Ministry of Defence (BMVg), while the Federal Intelligence Service (BfV) collects and evaluates information about terrorist-motivated cyber-attacks.[146, 147]

[146] Bundesministerium des Innern und für Heimat (2021)

[147] Bundesamt für Sicherheit in der Informationstechnik (2023b)

National authorities: BSI and BNetzA

The regulation authorities BSI and BNetzA, briefly introduced in Section 3.1, are decisive for the cybersecurity management of operators in the German electrical energy sector.

The BSI specifies cybersecurity standards and guidelines and conducts conformity testing of IT products to ensure they meet these standards. It serves as the single point of contact for the registration of assets and operators and for the reporting of cybersecurity incidents, which requires the appointment of a security officer within the company. Relevant reports and registrations are directly forwarded to the BNetzA. The BSI also performs a two-year verification of implemented security controls to ensure their compliance and effectiveness. The BSI provides ongoing notification of emerging and critical cyber threats, helping them stay aware of potential risks, and publishes information on hardware and software vulnerabilities as well as corresponding advisories. The BSI operates a situational awareness centre, which provides sector-specific computer emergency response teams (CERTs) within the CERT-Bund[148] and acts as a single point of contact for both preventive and reactive measures in case of cybersecurity incidents. Furthermore, the BSI operates the national crisis reaction centre for handling major cybersecurity incidents.[148, 149, 150]

Figure 9 illustrates the tasks of the BSI and its ties with other authorities.

The BNetzA is responsible for the security requirements of infrastructures, plants and operators in the electrical energy sector (e.g., by introducing IT security catalogues for energy plant operators[151] and grid operators[152]). This is accompanied by additional reporting and registration obligations, which in part differ from the BSI requirements.[153]

Additionally, the National Cyber Defence Centre (Cyber-AZ) is a platform across different national authorities (e.g., BMWK, BMI, BSI) to enable the rapid exchange of information and to implement protective measures to ensure cybersecurity in Germany.[154]

Non-governmental institutions and contact points

The CERT-Bund is the central point of contact for preventive and reactive measures in case of security incidents and has strong connections to the situational awareness centre and the national crisis reaction centre of the BSI. Similar to the BSI, the CERT-Bund issues information about hardware and software vulnerabilities as well as advisories.

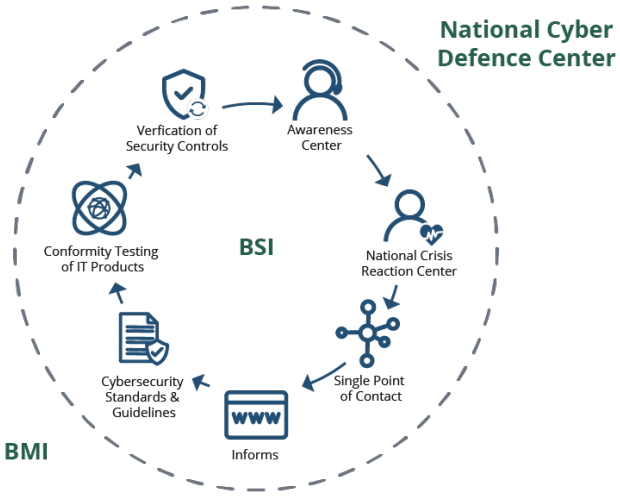


Figure 9: Roles, tasks and relationships of the BSI

Apart from the national authorities, there also exist several networks and institutions for information sharing and support services regarding cybersecurity in the private and industrial sector:

- The Alliance for Cybersecurity (ACS) enables information sharing (together with BSI) and networking on the topics: cyber threats, security controls and incident management[155].
- The Cybersecurity Network (CSN) is an association of qualified experts to establish a 'digital rescue chain' for incident handling. It also serves as a first point of contact for small or medium-sized companies and supports the exchange of experience[155].
- Transfer Point Cybersecurity (TISiM) was created by the BMWK to provide information, guidelines and best practices for cybersecurity in the SME sector[155].

[148] Bundesamt für Sicherheit in der Informationstechnik (2021)
[149] Bundesamt für Sicherheit in der Informationstechnik (2023a)
[150] OpenKRITIS (2024)
[151] Bundesnetzagentur (2025e)
[152] Bundesnetzagentur (2025f)
[153] Bundesnetzagentur (2024)
[154] Nationales Cyber-Abwehrzentrum, 2024
[155] David (2022)

- Sector Platform Cybersecurity in the Electricity Industry has been initiated by dena and founded by BMWK as an information sharing and knowledge platform for different actors in the electricity, digital and cybersecurity industries. Its aim is to anticipate upcoming problems within the German energy transition and identify common developments in terms of preventive measures and fields of actions.[156]
- The IT Security Association Germany (TeleTrust) is a competence network including domestic and foreign participants from a number of industries, administrations, consultancies and the sciences.[157]
- The Transfer Office for Cybersecurity in the SME sector ('CYBERsicher') supports SMEs, craft businesses and start-ups in the prevention and detection of as well as the reaction to cyber-attacks, including online tools to assess the cybersecurity status and emergency contact points.[158]
- UP KRITIS is a public-private partnership between critical infrastructure operators, initiatives and national authorities and operates under the BSI. Work at UP KRITIS is organised within and across the different sectors (including electrical energy) in Germany to prepare for and mitigate security incidents and supply failures. Relevant goals of UP KRITIS include the implementation of critical infrastructure regulations, the assessment of cybersecurity situations and crises and the establishment of crisis management structures.[159]
- CyberRange-e, launched in 2019 by E.ON, is a training centre for system operators where they can test and improve their capability to cope with IT- and OT-related cyber incidents.[160]

There are many information sharing platforms and contact points, in particular for the energy sector, including expert forums and associations[161].

5.1.2 Israel

Israel is considered one of the leading countries in the field of cyber protection and information security and places great store in maintaining technological superiority, especially vis-à-vis enemy states or organisations. Israel pursues a proactive cyber defence strategy, maintaining robust ties with US agencies. Thanks to strong links between the civilian and military cyberspace sectors, the domestic intelligence services, Shin Bet and Mossad, enhance cybersecurity through information sharing with state authorities and public bodies.[162, 163]

General cybersecurity architecture

The Israeli cybersecurity architecture is centralised under the INCD and the Israel Defence Forces (IDF). As previously referenced in Section 3.1, the INCD is responsible for cyber defence in the civilian sector and at public bodies. Conversely, the IDF is responsible for cyber offence, managing sophisticated cyber-attacks and espionage campaigns against enemy states (e.g., Iran) or organisations. Here, Unit 8200 (the Central Collection Unit of the Intelligence Corps) carries out offensive cyber operations and the C4I (command, control, computers, communications and intelligence) directorate acts to deter or pre-empt cyber-attacks as part of active cyber defence measures. Critical infrastructures are under the direct supervision of sector-specific regulators, with the added involvement of domestic intelligence services (e.g., Shin Bet).[163, 164]

National authorities: INCD and MoE

As outlined in the 2018 cybersecurity draft bill, the INCD is responsible for the national-level implementation and regulation of the national cyber strategy, which includes responding to national-level cyber-attacks. The INCD publishes cybersecurity policies and regulations aimed at protecting civilian cyberspace from various threats and vulnerabilities. Moreover, it strengthens emergency response capabilities to effectively address cybersecurity incidents and crises. As an example, the INCD provides and maintains the online YUVAL system[165] as a unique cyber calculator to assess the level of cyber protection in organisations and their compliance with local and international standards, with special focus on supply chain security. Within the national critical infrastructure protection (CIP), the INCD oversees the strategic policy planning and ensures the protection of public or governmental entities,

[156] dena Future Energy Lab (2024)
[157] TeleTrusT - Bundesverband IT-Sicherheit e.V. (2024)
[158] CYBERsicher (2024)
[159] Bundesamt für Sicherheit in der Informationstechnik (2022a)
[160] UNITY Consulting & Innovation (2025)
[161] Workshop (2024)
[162] Weinstock and Elran (2017)
[163] Frei (2020)
[164] Housen-Couriel (2017)
[165] Gov IL (2024e)

including the IEC, system operators (e.g., Noga) and others (defined in the Law of Regulation of Security in Public Bodies[166]). It also establishes and reinforces the cyber science-and-technology base, supporting academic research and fostering the cyber industry. Examples include the ACD portal[167] as a collaboration with Amazon to provide self-service protection services portal for SMEs and Cybershield[168] as a collaboration with Google to build a national monitoring infrastructure for the identification of cyber incidents in different sectors of the Israeli economy.[169, 170, 171, 172, 173, 174]

The INCD operates a centre for cyber incident management within the Israeli Cyber Emergency Response Team (CERT-IL)[175]. Established in the CyberSpark[176] complex in 2014, it provides continuous reporting and coordination between the INCD, public bodies and privatised public entities. The CERT-IL addresses various cyber incidents such as website defacements, social network hacking, phishing messages, DoS attacks, ransom attacks, information leaks, wiper attacks and impersonating pages. Additionally, it offers support for recovery and investigation of these incidents, receives and analyses digital artefacts and disseminates methods to improve response strategies. The CERT-IL engages in intelligence sharing with trusted partners both in Israel and internationally, actively promotes cybersecurity awareness across different sectors and advocates for the adoption of cybersecurity best practices. Furthermore, it serves as a single point of contact for threats and incidents affecting all civilian non-critical sectors.[171, 172]

Figure 10 illustrates the tasks performed by the INCD and its links with other authorities.

During Operation Iron Swords, the INCD's activities increasingly came to the fore and grew in terms of their impact. The agency is empowered to enact temporary orders that enhance its operational capabilities and increase its authority across various sectors. This includes coordinating cross-sector activities to reduce attack surfaces, particularly among controllers in the energy field. The INCD works to enhance resilience in critical supply chains and across approximately 150 local authorities, ensuring that preparedness is raised throughout the economy. Additionally, it investigates terrorist financing to mitigate risks that could exploit vulnerabilities during conflict.[177]

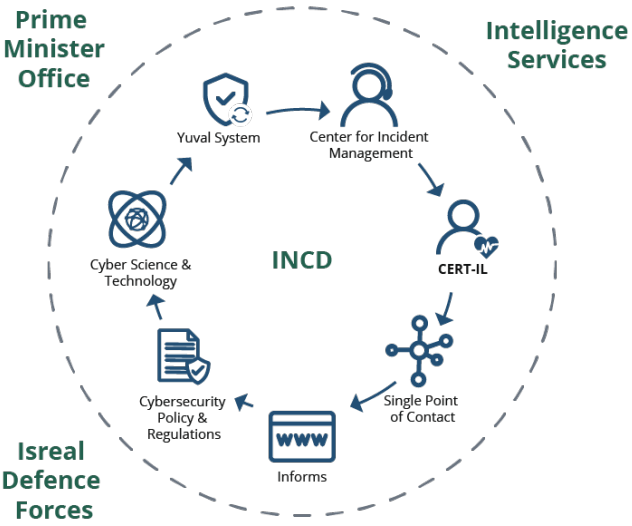


Figure 10: Roles, tasks and relationships of the INCD

[166] Nevo (2024)
[167] ACD/Labs (2024)
[168] Cybertech (2025)
[169] Takaharu (2022)
[170] Gov IL (2024f)
[171] Frei (2020)
[172] Housen-Couriel (2017)
[173] Stancu and Pavel (2023)
[174] Gov IL (2024c)
[175] Gov IL (2024g)
[176] Gav-Yam Negev (2024)
[177] Israel National Cyber Directorate (2023)

The Department of Emergency, Security, Information and Cyber within the MoE ensures the supply and functional continuity of the energy and water sectors, including the electricity, water and gas infrastructures. It prepares the MoE for upcoming cyber threats. For the energy sector in particular, a sector-specific cybersecurity unit within the MoE is responsible for the cybersecurity regulation and monitoring. In 2018, the MoE established a sector steering centre to monitor and control the critical infrastructures. This centre is now part of the MoE's Department of Sectoral Cybersecurity.[178]

The National Emergency Management Authority (NEMA) within the Israeli Ministry of Defence is responsible for home-front defence during emergency scenarios. The NEMA carries out exercises in conjunction with the IDF to handle cyber-attacks targeting critical infrastructures (e.g., the national electricity grid).[179, 180]

Non-governmental institutions and contact points

Israel has made substantial investments in civilian cyber capabilities, with around 200 to 250 cybersecurity start-ups and 20 research and development centres fostering innovation in the sector. Collaborative foundations between Israel and the United States promote shared cybersecurity initiatives and research, contributing to Israel's robust cybersecurity framework and its position as a global leader in the field.[181, 182]

The ICS National Cybersecurity Laboratory was established by the MoE and the INCD in 2017 as an international innovation and knowledge centre for cybersecurity in ICS environments. The laboratory serves government, academia, industry and military experts and investigates the effectiveness and capabilities of ICS products. Other activities include training and guidance of control system personnel in energy and water sector.[183]

Apart from the national authorities, there are several networks and institutions for information sharing that provide support services regarding cybersecurity in the private and industry sector:

- CyberNet is an information sharing platform set up by the INCD as part of a public-private partnership. It functions like a social network and includes over 1,000 cyber professionals (e.g., analysts, researchers) who use the platform to share information on cyber-attacks as well as other intelligence. Additionally, relevant cyber reports are sent to the CERT-IL team.[184, 185]
- CyberSpark, the Israeli Cyber Innovation Arena in Be'er-Sheva, is a public-private cyber defence partnership platform as well as a high-profile project that includes companies like Oracle, Lockheed Martin, IBM and Deutsche Telekom. A new IDF C4I branch tech campus was established in 2022, Additionally, two cyber innovation laboratories will also be set up for the energy and financial sectors.[181, 182, 186]
- Advanced Technology Park (ATP), housed on the campus of Ben-Gurion University in Be'er-Sheba, is a space for government officials, academics, corporations and the IDF to initiate projects and share information.[182]

Additionally, social networks are used as flexible platforms to directly exchange intelligence information in an efficient and anonymous way.[187]

[178] Gov IL (2024h)
[179] Ministry of Defense (2024)
[180] Housen-Couriel (2017)
[181] Frei (2020)
[182] Cohen et al. (2015)
[183] Gov IL (2024i)
[184] Frei (2020)
[185] Gov IL (2024j)
[186] Gav-Yam Negev (2024)
[187] Workshop (2024)

5.2 Cyber threat situation

5.2.1 Germany

As referenced in Section 3.1, the German electrical energy sector is highly decentralised and deeply integrated with neighbouring countries within the framework of the trans-European electricity grid. The diverse mix of energy generation capacity, which includes fossil and renewable energy sources, as well as the extensive integration of energy storage systems enable a high level of flexibility in the provision of energy and reduce dependence on large central power plants. While this enhances the system's ability to withstand widespread power outages, it also expands the number of potential access points for cyber attackers. This is particularly concerning given the numerous small, local energy providers and RES installations. Table 6 gives an overview of the reported cyber incidents in 2023 for the different German critical infrastructure sectors.

Table 6: Reported cyber incidents in Germany's critical infrastructure (KRITIS) sector in 2023[191]

Sector	Energy	ICT	Transport	Health	Water	Food	Finance	*Total*
Number of incidents	99	81	111	132	16	9	61	490

Relevant cyber threat scenarios

A couple of relevant cyber threat scenarios have been identified for the German electrical energy sector. This includes phishing e-mails sent at the enterprise level, where attackers seek to broaden the scope of the attack up to the operations management or process control level at the company. In doing so, they can take control over OT components (e.g., by exploiting the lack of or weak authentication and authorisation measures) and introduce false control signals using C&C servers. While the initial impact may be minor, these attacks can cause critical follow-up actions on the system resulting in potential long-term damage to equipment. Also, the exploitation of vulnerabilities in maintenance software (e.g., by infecting the smartphones of employees) allows attackers to establish persistent remote access. This opens up a direct entry point for cyber-attacks on critical assets with drastic consequences ranging from service disruptions to damage to facilities.[188, 189, 190, 191, 192]

Especially for smart meter systems, injection of malware into firmware can be used to establish a botnet and launch a mass disconnection of smart meters. This can cause the loss of wide area monitoring and billing functionalities with negative impact on market processes and overall power system stability.[193]

APTs targeting distribution systems

Distribution systems and DSOs have been identified as a valuable target for threat actors due to their responsibility for large energy supply areas and the increased use of digital technologies (e.g., wireless networks). Advanced persistent threats (APTs) are complex, multi-stage cyber-attacks, which are planned over long time periods to specifically target critical infrastructures. The initial stage starts with the reconnaissance of communication links or ancillary systems to gain remote access to DSO components. In subsequent stages the attacker can launch a sequential tripping of (previously identified) critical feeders, which leads to severe loss of and disruptions to energy production. APTs typically lead to multiple IT and OT systems being compromised over a long period of time, resulting in costly and extensive efforts to restore the systems. They have been partly observed in real installations.

[188] Petersen et al. (2023)
[189] Fischer et al. (2018)
[190] Bundesamt für Sicherheit in der Informationstechnik (2022b)
[191] Bundesamt für Sicherheit in der Informationstechnik (2023b)
[192] BDEW (2023b)
[193] Kreutzmann and Vollmer (2014)

Cyber threats targeting manufacturers and providers

As previously referenced in Section 2.3, supply chain attacks exploit the strong relationships and dependencies between client companies and suppliers or manufacturers in order to cause extensive damage in wide areas of the industry while remaining undetected for long periods of time. Also in the energy sector, these types of cyber-attacks are very difficult to detect and can cause large-scale disruptions to energy production or supply and can cause large-scale damage to equipment. Since threat actors actively gather information about untreated vulnerabilities, proper management and handling of hardware and software vulnerabilities by manufacturers is vitally important. The injection of malware or software vulnerabilities at an early stage of the supply chain (e.g., during production) may allow attackers to gain unauthorised access and execute malicious code upstream in the supply chain. In the case of relay firmware, backdoors introduced here can be used to change relay settings or setpoints for a large number of controllers simultaneously, which can have catastrophic effects on large energy supply areas and can lead to massive equipment damage. Alternatively, supply chain attacks can target remote access points of manufacturers and providers, which are used for maintenance and configuration tasks. Here, attackers can directly attack the remote access points using brute force methods and web-based injections or can indirectly attack the third-party IT systems by stealing credentials, certificates or (mobile) maintenance devices. As also discussed in the previous paragraph, attackers can then drop malware or further spread out in the network, especially in distribution systems. As a consequence, the ongoing use of external service providers and remote services (e.g., for maintenance tasks) in the energy sector opens up potential entry points for these kinds of cyber-attacks and requires comprehensive cybersecurity protection measures.[194, 195, 196, 197, 198, 199]

As a prominent example, in March 2022 (subsequently reported in April 2022) the German wind power plant manufacturer Nordex was hit by a ransomware attack (later claimed by the Conti cyber threat group). Detected at an early stage, this attack forced the shutdown of multiple internal IT systems and remote access points. Thus, the operation of wind turbine farms and their communication with system operators and energy traders were not further affected by the cyber incident.[200, 201, 202]

Cyber threats targeting OT legacy systems

Further major cyber risks arise for the energy sector from the use of legacy OT systems at the control level (e.g., SCADA systems) and at the field level (e.g., circuit breakers), which is associated with a low level of implemented security measures and controls (also see Section 2.3). These systems are characterised by limited support in terms of software updates, security patches and maintenance by the manufacturers as well as a lack of options to implement effective cybersecurity measures like endpoint protection and response. In particular, threat actors collect and use technical background knowledge and invest in long-term preparations to develop malicious code that is explicitly designed to harm and compromise ICS components (ICS malware). Particularly high cyber risks arise from the use of end-of-support (EoS) systems in ICS environments that lack bugfixes and security patches issued by the manufacturers. The replacement of these EoS systems can be extremely difficult owing to technical, operational or economic issues. In addition, malware code to exploit vulnerabilities in EoS systems is often publicly available and can be implemented easily by threat actors. Prominent examples of ICS malware include Stuxnet[203] (2010), a malware used to manipulate the frequency controller in Siemens SCADA systems; Havex[204] (2013), a malware used to eavesdrop on ICS systems; the BlackEnergy (2016) attack that used a modified ICS firmware to trigger large-scale energy supply disruptions; Industroyer[205] (2016), a malware used to open circuit breakers in substations; Triton[206] (2017), a malware used to disable industrial safety systems; and Incontroller[207] (2022), a malware used to scan ICS networks. [208, 209, 210, 211]

---

[194] Petersen et al. (2023)
[195] Fischer et al. (2018)
[196] Bundesamt für Sicherheit in der Informationstechnik (2022b)
[197] BDEW (2023b)
[198] Workshop
[199] Bundesamt für Sicherheit in der Informationstechnik (BSI) (2018)
[200] Arghire (2022)
[201] David (2022)
[202] Paganini (2022)
[203] Kapersky (2025)
[204] FKIE (2025a)
[205] FKIE (2025b)
[206] FKIE (2025d)
[207] MITRE ATT&CK (2024c)
[208] Petersen et al. (2023)
[209] Bundesamt für Sicherheit in der Informationstechnik (2022b)
[210] Workshop (2024)
[211] Bundesamt für Sicherheit in der Informationstechnik (2021)

As part of the ongoing process of IT/OT convergence (also see Chapter 2), the increased linking of OT and IT networks via Ethernet connections with insufficient documentation and protection can introduce additional entry points for attackers. There is an increase in the use of (mostly cloud-based) services from external providers to enable or support data acquisition and processing functions (e.g., for complex model calculations). This reduces costs and increases the redundancy and scalability of OT systems, especially for SMEs, but also leads to high risks in case of disrupted cloud connections (e.g., owing to DoS attacks) affecting a large number of OT systems and devices.[208, 209]

5.2.2 Israel

From Section 3.1, Israel's cybersecurity situation is shaped by its unique geopolitical landscape, characterised by long-standing threats to its national security with an ongoing shift towards cyber warfare. With numerous hostile neighbouring states (e.g., Iran) and terrorist organisations possessing advanced cyber capabilities, Israel faces a persistent and critical cybersecurity challenge. Furthermore, its geographical isolation as a 'desert island' exacerbates vulnerabilities, particularly in terms of the energy infrastructure. The lack of energy sharing with surrounding countries increases the risk of cyber-attacks targeting vital energy resources, making robust cybersecurity measures essential for national resilience.

Iranian threat actors and Operation Iron Swords

Iran has emerged as a highly active threat actor in the cybersecurity landscape, significantly developing its attack capabilities over the past decade. Notably, the Iranian hacking group APT33[212] has been involved in breaching various sectors, including infrastructure, banking, aerospace and the petrochemical industry, utilising a complex Trojan program known as 'DROPSHOT'. APT33 has executed cyber network attack (CNA) and cyber network exploitation (CNE) operations against entities such as Shin Bet, the Ministry of Defence and the Bank of Jerusalem. Additionally, Iran has begun targeting critical infrastructures, specifically the water, power and financial sectors, to enhance its cyber warfare strategy. Furthermore, Iran has been cooperating with Hamas to support cyber operations, indicating a collaborative approach to enhancing its offensive cyber capabilities.[213, 214, 215, 216]

Especially during Operation Iron Swords, the number and extent of cyber threat activities has increased significantly (2.5 times more incidents than usual). This took the form of 500 inquiries per day (ten times more than usual) and a 43 per cent increase in incident reports compared to 2022. Figure 11 highlights the main cyber threat activities during Operation Iron Swords, while Figure 12 shows the number of reported cyber incidents in 2023.

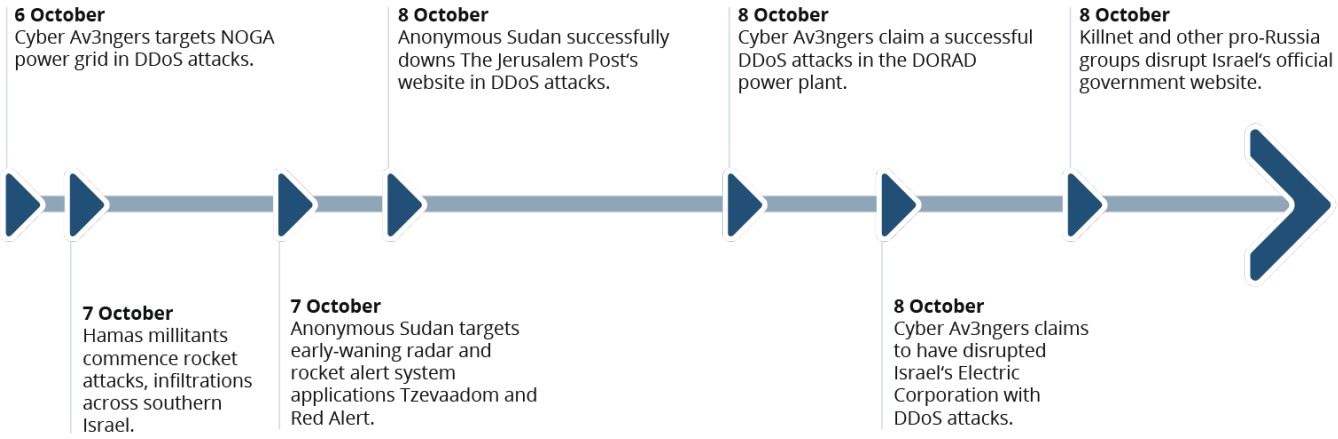


Figure 11: Timeline of relevant cyber threat activities during Operation Iron Swords[217]

[212] MITRE ATT&CK (2024d)
[213] Cohen (2019)
[214] Cohen et al. (2015)
[215] Israel National Cyber Directorate (INCD) (2024)
[216] Mizrahi et al. (2024)
[217] Buckley et al. (2023)

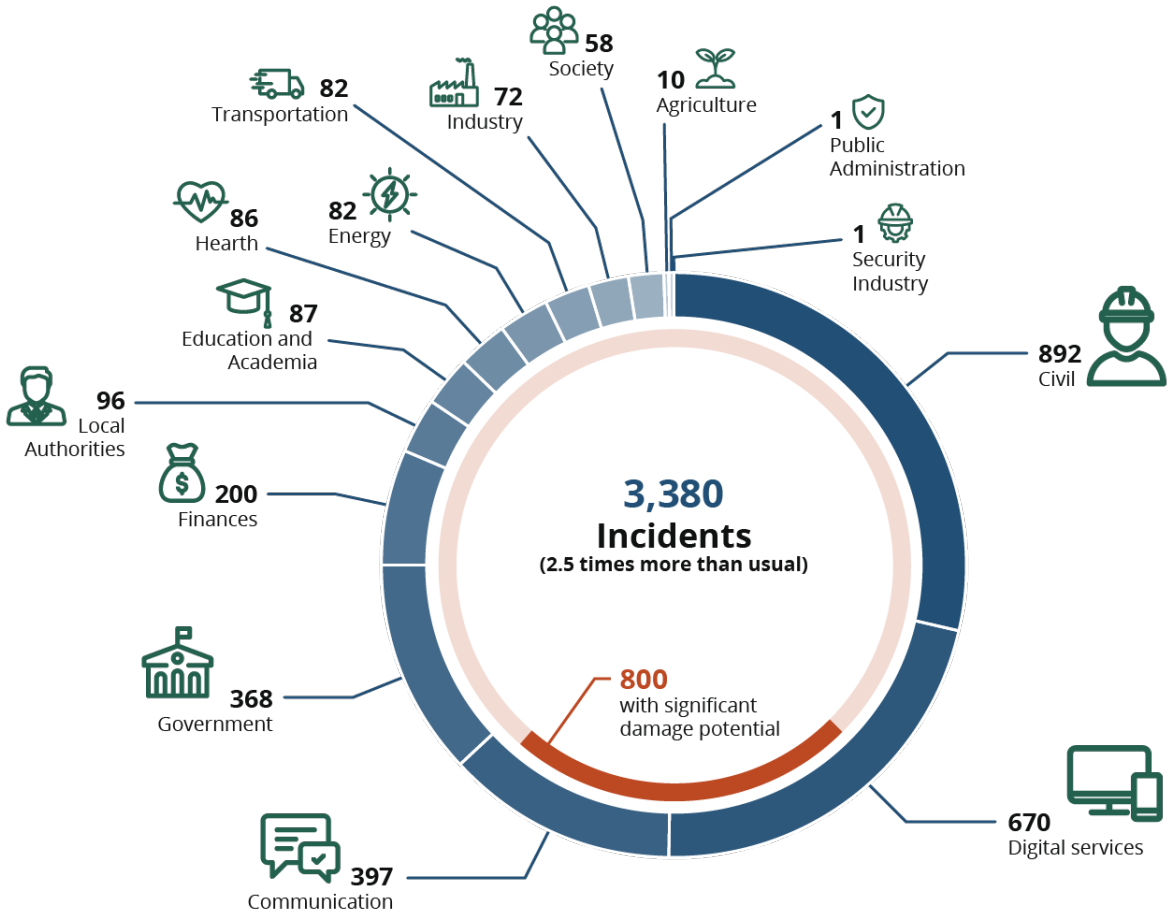


Figure 12: Number of reported cyber incidents during Operation Iron Swords in 2023[218]

[218] Israel National Cyber Directorate (2023)

Fifteen main attack groups have been identified by the INCD that are associated with Iran, Hamas and Hezbollah that share intelligence, methods and attack tools. Most threat actors employ lower-level capabilities, including DDoS attacks, website defacements, doxing attacks, online shaming or disinformation (via social networks). Specific cyber-attacks have been observed that target Linux systems, Internet-connected security cameras, IoT and mobile devices (e.g., smartphones), and managed service providers.[215, 219]

General cyber threats and vulnerabilities

For 2023, the INCD identified a number of core vulnerabilities, including web shells on exchange servers, outdated versions of file editors (e.g., FCKeditor or TinyMCE) as well as software weaknesses in VPN components and file upload interfaces. The most attacked assets include PLC interfaces, IoT devices and web servers or interfaces. In general, cyber threats against Israel shift from CNE to CNA (e.g., destructive deletion attacks) and target 'hub' organisations. There has been a significant increase in ransomware attacks, especially to destroy network information (wiper-type attacks). Here, manufacturers are a preferred target for ransomware groups (e.g., 21 per cent of ransomware attacks in 2024 focused on production environments) due to a lack of adherence to security updates and the widespread use of legacy technologies. Ransom-as-a-service tools have been discovered by cyber threat actors as a new business model.[220]

Additionally, the INCD is highly focused on cyber-attacks perpetrated on ERP systems, where malware (e.g., the Trojan program DEX) is used to impair banking or SAP systems in order to expose sensitive information (e.g., customer data, conduct data) or to disrupt essential business processes[221]. Another important cyber threat is supply chain attacks, which according to the INCD are considered as highly relevant for companies and organisations. In 2022, the INCD reported an increase of approximately 65 per cent in such attacks, mainly affecting service providers and suppliers.[222]

Furthermore, malice actions of employees and remote access over the Internet in order to gain entry to an organisation's network are seen as major entry points for attackers. This includes e-mails containing infected links or attachments and embedded hostile code, communication gateways infiltrated using administrator privileges or the infection of workstations.[223]

Existing and potential cyber threats in the energy sector

In the recent past, several cyber-attacks have been observed in the Israeli energy sector, including multiple large-scale attacks against power sites by Iran, Hamas and Hezbollah in 2013[224] as well as a ransomware attack against the PUA in 2016[225]. The CERT-IL details an attack campaign in 2019[226] against Israeli organisations, including those operating in the energy sector. Here, the perpetrators launched attacks against web servers, RDP/VPN connections and OWA/DNS servers.

A study[227] identified DDoS attacks, backdoor attacks from corrupted supply chains, spear phishing e-mails and malware attacks as relevant cyber threat scenarios. Also from a military perspective, long electromagnetic pulse (EMP) attacks are seen as a key physical threat against different assets of the Israeli energy sector[227, 228]. Here, restoring the power system is highly contingent on being able to return transformers, relays and stations back to operation. As in case of Germany, the long software and hardware update cycles and high-performance requirements of OT devices pose a serious cyber threat to the Israeli energy sector.[228]

5.3 Cybersecurity indicators

Based on the findings from Sections 5.1 and 5.2, several cybersecurity indicators and metrics have been derived to assess and compare the state of cybersecurity in Germany and Israel. This is done by analysing the roles and tasks of existing national authorities and non-governmental institutions as well as the criticality of relevant cyber threats and the associated exploitation of systemic weaknesses. Table 7 lists the defined cybersecurity indicators and chosen metrics for this study.

[219] Buckley et al. (2023)
[220] Israel National Cyber Directorate (2024b)
[221] Israel National Cyber Directorate (2019a)
[222] Israel National Cyber Directorate (2024c)
[223] Israel National Cyber Directorate (2021)
[224] Cohen et al. (2015)
[225] Brook (2016)
[226] Israel National Cyber Directorate (2019b)
[227] Weinstock and Elran (2017)
[228] Workshop (2024)

Table 7: Overview of defined cybersecurity indicators

Indicator	Basis for assessment (metric)
National authorities	
Specification of security policies or regulations	• Scope and the goal of the specification • Actors in the energy sector affected by specified policies or regulations
Supervision of implemented security controls	• Nature of supervision (e.g., audits, conformity testing) • Supervised actors in the energy sector • Use of punitive measures
Reporting (e.g., asset registration, incidents)	• Type of items to be reported • Affected actors in the energy sector that report
Support for security controls or incident handling	• Focus of support and support services offered • Actors in the energy sector to be supported
Information sharing (e.g., cyber threats, warnings, vulnerabilities, advisories)	• Type of information shared • Actors in the energy sector with access to the information
Cooperation or competition between entities	• Existing fields of cooperation between authorities and other institutions • Existing fields of competition or responsibilities between different authorities
Non-governmental institutions or associations	
Support for security controls or incident handling	• Focus of support and support services offered • Actors in the energy sector to be supported
Information sharing (e.g., cyber threats, warnings, vulnerabilities, advisories)	• Type of information shared • Actors in the energy sector with access to the information
Cooperation with national authorities	• Existing cooperations with national authorities
Cyber threat situation	
Cyber incidents	• Number of reported cyber incidents
Threat extent and criticality	• Actors in or areas of the electrical energy sector affected by the cyber threat • Impact and consequences exhibited by the cyber threat on the system
System susceptibility and weakness	• Systematic weaknesses or potential vulnerabilities exploited by the cyber threat

6 Comparative analysis: similarities and differences

The digitalisation of power grids in Germany and Israel highlights both similarities and strong differences in their approaches to modernising energy infrastructure. As referenced in Chapter 3, the German energy transition leads to a highly decentralised energy system with a high proportion of wind and solar energy installations, the downside of this being a high number of possible entry points for cyber threat actors at the transmission and distribution level. For Israel, on the other hand, the handling of physical and cyber threats has utmost national priority within a proactive cyber defence strategy. Israel's energy infrastructure is highly centralised, allowing for efficient deployment of smart metering technology, with the country's grid being linked to neighbouring countries ('desert island') only to a very limited extent. As both countries aim to create more efficient and resilient energy systems, they face distinct challenges shaped by their unique energy landscapes, regulatory and technological frameworks, and strategic priorities.

Based on the findings from Chapter 4 and Chapter 5, this chapter summarises the main similarities and differences in the digitalisation efforts as well as in terms of the cybersecurity architecture and cyber threat situation of Germany and Israel within the energy sector. It highlights key areas of common innovations based on the identified challenges and inhibitors in each country. For this, Section 6.1 compares the quantitative and qualitative indicators including:

- the analysis of digitalisation indicators to assess energy market roles and potential business models, smart meter deployment, installed capacities and energy production by renewable energies as well as connection requests and digital supervision in the transmission and distribution system in Section 6.1.1; and
- the analysis of cybersecurity indicators to assess roles and tasks of national authorities, contact points and non-governmental institutions as well as the criticality and effect of relevant cyber threats and their exploitation of systemic weaknesses in Section 0.

Based on this comparative analysis, Section 6.2 derives common and specific challenges of digital advancements and cybersecurity efforts in the energy sectors of Germany and Israel. Additional workshops were held with different representatives from authorities and ministries in both countries to reflect and prioritise the relevant challenges and possible innovation fields.

6.1 Comparison of indicators

6.1.1 Digitalisation in GER and ISR

As referenced in previous chapters, Germany and Israel are both navigating the complex and transformative journey of digitalising their electrical grids, but they do so from vastly different starting points and also have significantly different strategic priorities. Germany's energy production is dominated by wind and solar plants, which produced a total of 53 per cent of RES-generated power in 2022. The German energy infrastructure is highly decentralised and divided amongst four TSOs and approx. 900 DSOs, with an ongoing smart meter rollout anchored in the German digital strategy. Since its foundation, Israel has been in a difficult geopolitical situation, making it a 'desert island' with no interconnections to surrounding countries. Israel's energy infrastructure is centralised under the IEC with a single TSO, and despite its high solar energy potential, generated only 11 per cent of its power from RESs in 2022.

Energy market and metering

Germany's progress in rolling out smart meters has been relatively slow. By 2022, only 11 per cent of electricity connections in the country were equipped with smart meters. The government has outlined a detailed plan to accelerate deployment, aiming for wider adoption by 2032, with a focus on larger consumers and renewable energy producers[229]. Current regulation requires consumers of more than 6.000 kWh/a (up to 100.000 kWh/a), producers starting at 7 kW, and owners of a controllable end-use device in accordance with § 14a of the EnWG (Such as heat pumps or BEV charging facilities) to install a smart meter. Consumers below this threshold will be fitted with digital meters that are not necessarily connected to communication systems.

In contrast, Israel has advanced more rapidly. Israel faces challenges in its smart meter rollout, having achieved only five per cent coverage by 2021; efforts to address this include importing smart meters from China, which are now being deployed, though concerns about their security and other potential issues remain under evaluation, with the rollout accelerating since 2022. The centralised structure of Israel's grid, managed by the IEC, has enabled a more streamlined and efficient rollout of advanced metering infrastructure relying heavily on standard or electronic meters[230]. Figure 13 (see below) shows the share of smart meters, digital meters and other meters in both countries. The numbers for Germany are conservatively based on current consumption and market penetration of generating units or controllable devices. Increased electrification of heating and mobility, as well as dynamic tariffs should lead to more widespread deployment of smart meters than is reflected in figure 13.

[229] FfE (2023)

[230] Enerdata (2024)

Smart meter deployment plans

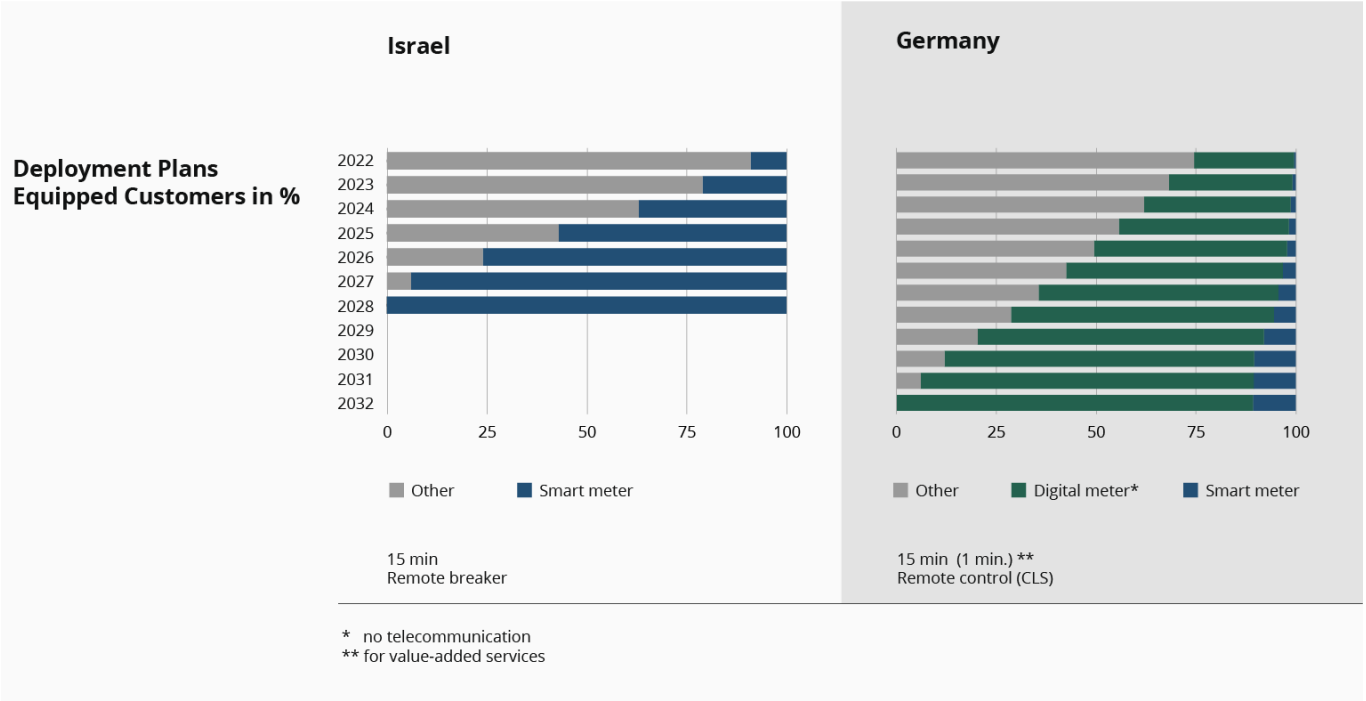


Figure 13: Comparison of digitalisation indicators for smart meters

The communication technologies underpinning smart meter infrastructure differ between the two countries. Germany's smart meters rely on a combination of LTE (71 per cent), power line communication (PLC, 14 per cent) and DSL (four per cent). Fibre optic networks are being expanded, but progress remains slow[231, 232]. Israel, on the other hand, uses more robust wired communication networks for smart meters, managed centrally by the IEC, ensuring greater reliability and security[233]; however importing most of its smart meters from China has the potential to open up security risks.

Distributed energy production

Germany's investment in renewable energy infrastructure is significantly higher than Israel's. By 2022, Germany had an impressive total installed renewable energy capacity of 150.4 GW, with substantial contributions from wind (59.3 GW onshore and 8.4 GW offshore) and solar power (73.97 GW). This translates to over 60 per cent of the country's total generation capacity[234]. Meanwhile, Israel's installed capacity of renewable energy remains relatively modest, focusing almost entirely on solar power, which accounts for about 20 per cent of its total installed capacity (approximately 3-4 GW)[235]. Figure 14 compares Germany's and Israel's installed generation capacities.

[231] Power Plus Communications AG (2020)
[232] Devolo AG (2019)
[233] Mesicek (2023)
[234] Fraunhofer Institute for Solar Energy Systems ISE (2025a)
[235] Proaktor et al. (2023)

Installed capacity and actual generation, 2023

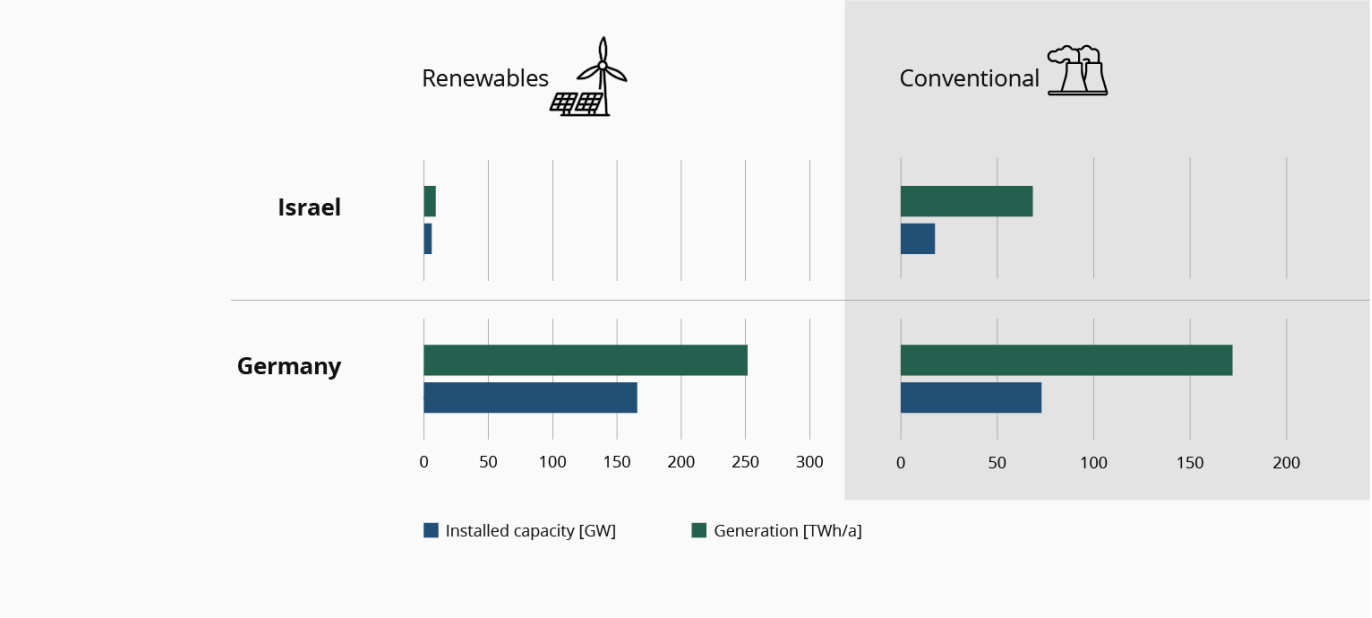


Figure 14: Comparison of digitalisation indicators for installed generation capacities

Despite these differences in capacity, the share of renewable energy in electricity generation tells a compelling story. In 2023, renewable energy sources (RESs) contributed around 53 per cent of Germany's electricity generation, a substantial increase from 41 per cent in 2022[236].

This is largely driven by wind farms and biomass, which are rare in Israel's generation portfolio. Israel, however, is rapidly expanding its solar energy production. By 2023, solar power constituted around 11 per cent of Israel's total electricity generation, marking a 33 per cent increase from the previous year[237].

Grid connection of new generators

Efficiency in connecting new renewable energy projects to the grid is another crucial metric. In Germany, regulations mandate that DSOs approve grid connection requests within eight weeks (56 days)[238]. While there is no comprehensive data to confirm compliance, this timeline is more favourable than in Israel. In Israel, the average response time for grid connection requests varies significantly: positive responses within 67 days, partially positive responses with 213 days (often requiring further information or capacity reduction measures), limited positive responses within 168 days and negative responses within 100 days. This extended timeline for more complex approvals in Israel underscores challenges in streamlining the integration of new energy projects[239]. Figure 15 summarises the comparison.

[236] Fraunhofer Institute for Solar Energy Systems ISE (2025b)
[237] Tsagas (2024)
[238] Bundesnetzagentur (2025g)
[239] Reuters (2024)

Grid connection requests, 2022

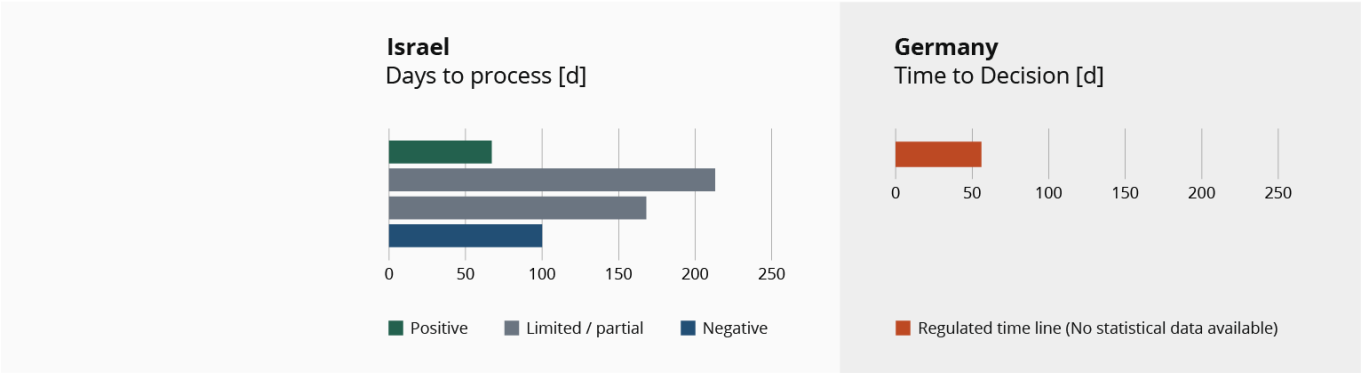


Figure 15: Comparison of digitalisation indicators for grid connection requests

Transmission and distribution system

Figure 16 highlights the differences in grid structures and investment priorities between Germany and Israel, focusing on voltage levels and expansion strategies. Germany's grid comprises approximately 2.2 million kilometres of distribution lines and 36,300 kilometres of transmission lines, with low voltage dominating both in terms of line length and grid share due to its role in residential and industrial distribution. In contrast, Israel emphasises high-voltage transmission to efficiently transport electricity from remote solar farms to urban centres, balancing investments across voltage levels to manage renewable energy variability.

Electrical grid, 2023

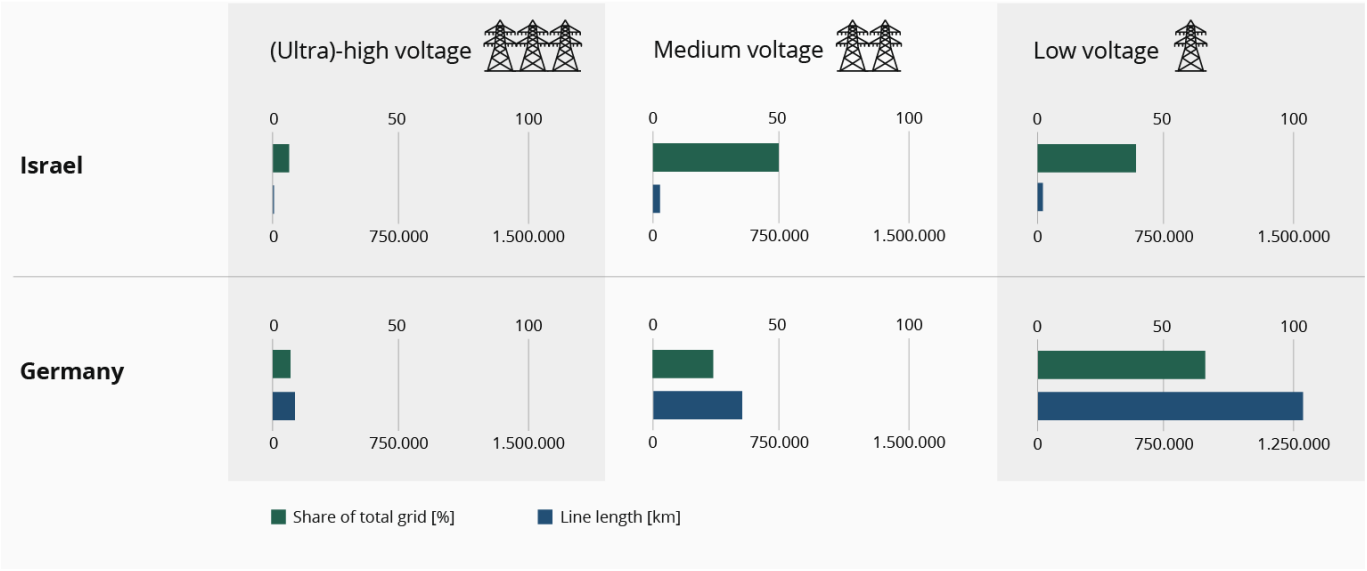


Figure 16: Comparison of grid line lengths for voltage levels

In Figure 17 the proposed expansion of grids is presented. Germany allocated €13.12 billion in 2022 to optimise its grid, targeting medium- and high-voltage reinforcement, congestion and curtailment of 8 TWh of renewable energy. Israel invested NIS 3 billion in 2021, focusing on high-voltage expansions and smart grid technologies to stabilise its increasing reliance on renewable energy. Proposed expansions by 2030 (Germany) and 2032 (Israel) further highlight Germany's focus on higher reinforcement percentages and cost allocation to medium- and high-voltage networks, while Israel adopts a more balanced grid upgrade approach.

Proposed expansion plans

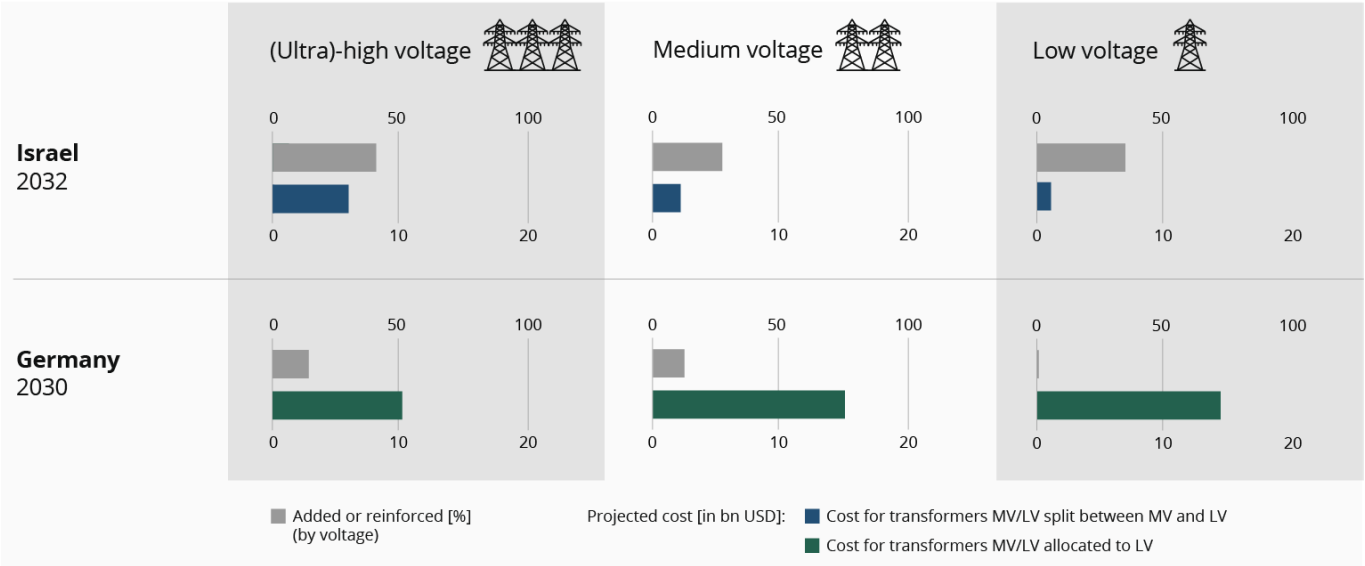


Figure 17: Proposed expansion of grids (including new lines, reinforced lines)

Germany and Israel also differ in the extent of digital supervision of their power grids. In Germany, high-voltage grids are highly digitalised, with real-time monitoring and advanced control systems. However, medium- and low-voltage networks, particularly in rural areas, lag behind in terms of digitalisation, and efforts to automate these networks are ongoing. Israel benefits from a more centralised and digitally supervised grid[240]. The IEC has implemented extensive real-time monitoring and automation, making grid operations more efficient and reliable compared to Germany's fragmented system[241].

Main similarities and differences

From these findings, a number of distinct similarities and differences can be identified between the German and Israeli energy sectors regarding smart meter penetration, renewable energy capacity and grid management efficiency.

The main similarities can be summarised as follows:

1. Both countries **utilise and focus heavily on solar energy** technologies to achieve a carbon-free energy supply, leading to 74 GW of installed capacities in Germany in 2022 (constituting 30 per cent of the total installed RES capacity) and 3-4 GW of installed capacities in Israel in 2022 (constituting 20 per cent of the total installed RES capacity). This reliance on solar energy increases the integration of digital technologies for efficient management and optimisation, making these systems susceptible to cyber-attacks targeting the supply chain, including vulnerabilities introduced through third-party vendors.
2. Germany and Israel **are advancing digital grid management through smart meters**, emphasising real-time monitoring, automation and efficient communication networks. Germany focuses on improving transparency, rural grid digitalisation and market data access, while Israel leverages centralised digital supervision for enhanced grid efficiency and reliability. Both countries, while lagging behind in terms of smart meter rollout compared to other European countries, enable value-added services like dynamic pricing, demand response programmes and actionable energy consumption insights, driving efficiency and consumer empowerment[242]. However, the increasing ICT penetration and inter-connectivity expose these grids to cybersecurity threats, requiring robust protective measures and secure communication protocols.
3. Israel has achieved 20 per cent overall smart meter coverage, while Germany's smart meter coverage stands at 10.9 per cent. However**, both countries lag behind the global average** and many European nations, highlighting the need for accelerated deployment and alignment with international benchmarks.
4. Both Germany and Israel are working on integrating DERs such as PV systems, wind turbines, battery energy storage systems (BESS), microgrids, electric vehicles with vehicle-to-grid (V2G) technology, combined heat and power (CHP) systems and biogas units, to **diversify and decentralise electricity production**, supporting their national energy transition goals. This integration depends on advanced digital systems for coordination and optimisation, making the grid more resilient yet more vulnerable to cyber-attacks targeting DER communication and control systems, underscoring the need for secure digital infrastructures and comprehensive risk management strategies.

Conversely, the main differences can be summarised as follows:

1. Germany has **high installed capacities of wind and solar energy plants** while also expanding into biomass and hydroelectric power. As a result, **53 per cent of electricity was generated from renewables** in 2023. Israel focuses primarily on solar energy, providing 11 per cent of electricity production from renewables.
2. Israel's higher solar irradiance results in greater **efficiency in solar energy generation** (5.08 kWh/kWp) compared to Germany (2.96 kWh/kWp).
3. German DSOs are required to **approve grid connection requests within 56 days**, whereas Israel's grid connection approval times are long and vary significantly based on the complexity.
4. Germany's energy sector uses a mix **of LTE, PLC and DSL** communication, while Israel relies on **robust wired communication networks** managed by the IEC.

[240] Euractiv (2023)
[241] POWERGRID International (2025)
[242] Israel Energy Partnership (2025)

6.1.2 Cybersecurity in GER and ISR

As referenced in previous chapters, Germany and Israel are both facing severe challenges in dealing with cyber threats increasingly targeting actors in energy infrastructures (e.g., in the form of ransomware attacks). This is especially true regarding the protection of OT systems and supply chains as this relates to manufacturers and external service providers. Germany's cybersecurity landscape is primarily overseen by the BSI as the central authority for cybersecurity. Although only a few serious cyber incidents have been reported in the German electricity sector, the distribution system and DSOs in particular are at high risk from cyber threats, including APTs and supply chain attacks. Israel's cybersecurity strategy is characterised by a proactive cyber defence integrating military and civilian cyberspace efforts, whereby the INCD acts as the central authority for civilian cyber defence. The ongoing military operation, which goes under the name Iron Swords, in particular has led to a significant increase in cyber incidents targeting the energy sector. This results in a notable rise in cyber threats from enemy states (e.g., from Iranian cyber threat group APT33), with a strong shift in focus towards more destructive cyber-attacks.

As already mentioned in Section 1.4, the available information on cybersecurity is extremely limited as this pertains to the Israeli energy sector. Documents on sector-specific regulations, authorities and cyber threats are not publicly available. This can be justified by the much higher threat level in Israel, especially during Operation Iron Swords; this makes it difficult to fully compare the cybersecurity of the energy sectors in the two countries.

National authorities, institutions and associations

In Germany, the central authority BSI (together with the BNetzA) primarily regulates and supervises electrical grid and plant operators (e.g., via a two-year conformance verification), including support in the form of information, including guidelines, cyber threat warnings and advisories (this is a collaborative project in partnership with CERT-Bund). Cyber incidents must be reported to the BSI while providing sector-specific CERTs within the CERT-Bund. In Israel, the INCD performs similar roles to those carried out by Germany's BSI, while also providing intelligence, guidelines and other information. The INCD, sector-specific regulators as well as the MoE security department offer conformance verification (e.g., via the online system YUVAL). Cyber incidents must be reported to the CERT-IL (within the INCD) including sector-specific CERTs. Additionally, MoE's Sectoral Cybersecurity Division performs annual trainings including Tabletop Exercises for operators in the Israeli energy sector. Table 8 describes and compares the metrics for the cybersecurity indicators regarding the national authorities.

Table 8: Comparison of cybersecurity indicators for national authorities

	Israel	Germany
Specification of regulations	• Regulations for specific public-private bodies issued by the INCD • Sector-specific regulators • MoE's Cybersecurity Division	• Regulations for energy grid and plant operators issued by BSI • Security requirements for infrastructure and operators issued by BNetzA
Supervision of security controls	• YUVAL system: voluntary online conformance verification for organisations • MoE's Sectoral Cybersecurity Division oversees regulations including auditing	• Conformance testing of IT/OT products by BSI • Two-year verification of security controls by BSI
Reporting e.g., asset registration, incidents	• Electricity producers must report cyber incidents to the Ministry of Energy's sectoral CERT. • DSOs and TSOs report to INCD as well as the MoE CERT	• Registration of assets and operators by BSI/BNetzA • Cyber incidents reported to BSI/BNetzA
Support for security controls or incident handling	• MoE's Cybersecurity Division publishes sector specific regulations and guidelines as well as Cyber trainings	• BSI publishes guidelines and best practices • BSI provides sector-specific CERTs within CERT-Bund

	Israel	Germany
Information sharing e.g., cyber threats, warnings, vulnerabilities, advisories	• INCD provides vulnerabilities and advisories • INCD informs about cyber threat warnings	• BSI/CERT-Bund provides information on vulnerabilities and advisories • BSI issue notifications about cyber threat warnings
Cooperation or competition between entities	• The Ministry of Energy's Cybersecurity Division provides sector-specific vulnerability alerts, advisories, and cyber threat intelligence (CTI).	• Cyber-AZ coordinates activities of ministries • Competing obligations between BSI and BNetzA

Apart from the national authorities, actors in the Germany energy sector are supported in cyber incident handling by a variety of institutions and associations including the CSN, the Transfer Office for Cybersecurity, UP KRITIS and CyberRange-e. Other information sharing platforms and contact points exist, in particular for German SMEs; these include ACS, TISiM and TeleTrust. For operators in the Israeli energy sector, support in cyber incident handling encompasses sector-specific monitoring by Cybershield, control system training by the ICS National Cybersecurity Laboratory and protective services for SMEs offered via the ACD portal. Cybernet, ATP and social networks offer the opportunity for sharing information as well. In particular, Cyberspark is an internationally renowned technology park that supports cyber innovations and provides networking opportunities; companies like Oracle, Lockheed Martin, IBM and Deutsche Telekom are part of the network. Table 9 describes and compares the metrics for cybersecurity indicators for non-governmental institutions and associations.

Table 9: Comparison of cybersecurity indicators for non-governmental institutions and associations

	Israel	Germany
Support for security controls or in incident handling	• ACD portal: protective services for SMEs • Cybershield: sector-specific incident monitoring • ICS National Cybersecurity Lab: control system training, ICS product testing • Cyberspark: cyber innovation laboratory	• CSN: incident handling for SMEs • Transfer Office for Cybersecurity for security controls in the SME sector • UP KRITIS: incident and supply failure handling for critical infrastructure operators • CyberRange-e: training centre for system operators to assist in handling cyber incidents
Information sharing e.g., cyber threats, warnings, vulnerabilities, advisories	• Cyberpark: cyber defence platform for ministries and companies • CyberNet: social network with > 1,000 professionals • ATP: information sharing • Social networks	• ACS: threat information and incidents • TISiM: guidelines and best practices for SME sector • Sector platform cybersecurity: preventive measures • TeleTrust: competence network
Cooperation with national authorities	• INCD established ACD and Cybershield • Cyberspark created CERT-IL and IDF C4I campus • ICS National Cybersecurity Lab established by the INCD and MoE • CyberNet informs CERT-IL • ATP includes government officials and the IDF	• ACS cooperates with BSI • TISiM established by BMWK • Sector platform cybersecurity founded by BMWK • UP KRITIS under BSI

Cyber incidents and cyber threat situation

The national cybersecurity authorities, BSI and INCD, annually report the number of cyber incidents in relevant industrial sectors, including the energy sector. While the number of incidents in the energy (Germany: 99, Israel: 82) and transportation (Germany: 111, Israel: 82) sectors is quite similar in both countries, the finance sector in Israel (200) reports a significantly higher number of incidents compared to Germany (61). Nevertheless, a direct comparison of these numbers is not sufficient to assess the cyber threat situation in both countries. A fair comparison and analysis should consider more detailed information about the number of public and private bodies in both sectors, the requirements to report a cyber incident as well as the number of unreported and possible undetected cyber incidents.

Apart from the number of cyber incidents, several cyber threats in the German and Israeli energy sectors have been described in Section 5.2. Based on these findings, the following seven generic cyber-attack scenarios can be derived:

- ***Launch phishing e-mails* (T1);**
- ***Infiltrate maintenance access* (T2);**
- ***Inject malware (malicious code)* (T3);**
- ***Infiltrate communication gateways* (T4);**
- ***Attack supply chain components* (T5);**
- ***Launch ransomware* (T6); and**
- ***Launch an electromagnetic pulse (EMP)* (T7).**

These cyber-attack scenarios address common system susceptibilities and weaknesses in the German and Israeli energy sectors. These include unsecure mail clients and insufficient awareness or malice activity (T1), unsecure and outdated software (T2, T3, T7), insufficient protection of mobile devices (T2), remote access points (T2, T5), communication (T4), lack of checks regarding external providers (T5), insufficient physical protection or countermeasures against EMP (T6) and insufficient backup capabilities (T7).

For a corresponding qualitative assessment of the extent and criticality of these attack scenarios on the energy supply, the potential consequences of the cyber-attack scenarios are roughly divided into the following five categories:

- Follow-up effect from cyber-attacks that exhibit no direct impact on the energy supply but may lead to critical follow-up actions;
- *Local effect* from cyber-attacks disrupting the energy supply in small areas of the electrical grid or of a few large energy consumers;
- *Long-term* and local *effect* from cyber-attack disrupting the energy supply in small areas of the electrical grid or of a few large energy consumers, which may go undetected for a long period or may require a large amount of time and effort to restore service;
- *Large-scale effect* from cyber-attacks disrupting the energy supply in wide areas of the electrical grid endangering the power system's stability; and
- *Long-term* and *large-scale effect* from cyber-attacks disrupting the energy supply in wide areas of the electrical grid endangering the power system's stability, which may go undetected for a long period or may require a large amount of time and effort to restore service.

Considering these cyber-attack scenarios and the associated consequences, Figure 18 shows the results of the qualitative cyber threat assessment for the German and Israeli energy sectors. This assessment takes into account the different energy infrastructure and state of digitalisation (see Chapter 4) in both countries. The effects of the different cyber-attack scenarios are evaluated for the relevant areas of the energy sectors in this study, including energy producers, metering systems, external providers as well as transmission and distribution systems. For simplicity's sake, possible interactions or cascading effects between the different cyber-attack scenarios are not considered.

Cyber threats on German/Israeli energy sector

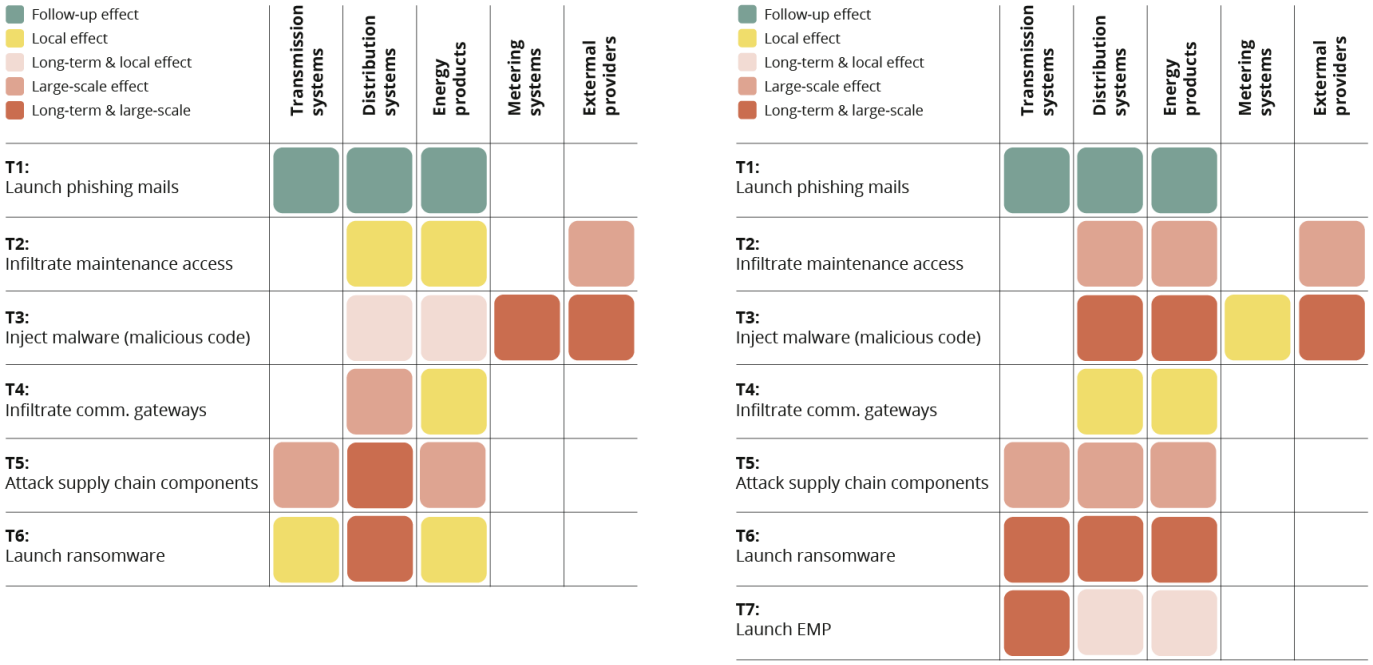


Figure 18: Extent and criticality of cyber threats in the German (left) and Israeli (right) energy sectors

Main similarities and differences

Based on these findings, a number of distinct similarities and differences can be identified in terms of the cybersecurity architecture and the cyber threat situation of the German and Israel energy sectors. The main similarities can be summarised as follows:

1. The cybersecurity architecture is characterised by **central cybersecurity authorities** (BSI and the INCD) with similar roles and tasks as well as the operation of sector-specific CERTs.
2. There are a **large number of information sharing and cybersecurity support platforms** available to companies (e.g., for publishing new software vulnerabilities and advisories as well as warnings about upcoming cyber threats; for supporting incident response and security control implementations).
3. **Ransomware and supply chain attacks** with phishing e-mails as a common entry point have been identified as common cyber threats that exhibit potential large-scale disruptive effects on the German and Israeli energy supply.
4. The **lack of checks and regulations with regards to manufacturers and service providers**, including insufficient protection of corresponding remote access points can be seen as systemic weaknesses in the German and Israeli energy sectors.

Conversely, the main differences can be summarised as follows:

1. In Germany's cybersecurity architecture of the different **ministries are coordinated by Cyber-AZ**. German institutions and associations in particular provide a wide range of information sharing and networking possibilities for SMEs.
2. The German energy infrastructure poses **a high risk in terms of cyber-attacks on the distribution system and on smart metering** systems (especially via malware injection).
3. The **insufficient protection of OT devices and the continued use of OT legacy systems** are major challenges in the German energy sector.
4. Israel's cybersecurity architecture is characterised by a **high level of funding and investment in start-ups and tech companies**. The **strong ties between the military and civilian cyberspace** leads to well-developed cooperation between public bodies, private organisations and intelligence services.
5. Israel's cybersecurity authorities (e.g., NEMA) require **emergency training for operators in the energy sector**, whereas in Germany similar emergency training is currently offered by private companies (e.g., CyberRange-e from E.ON).

6. Israel uses **social networks for efficient intelligence sharing** 'at the ground level' of cyber threat information.
7. Israel's special geopolitical situation and Operation Iron Swords result in an increased number of cyber incidents and an **ongoing shift to destructive attacks** (e.g., wiper-type ransomware). Especially high **risks arise from EMP attacks** as well **as large-scale effects from malware injection and ransomware attacks**.[243]
8. Unlike Germany, a lot of **information on cybersecurity in the Israeli energy sector is not disclosed or made publicly available**. This includes sector-specific information on specific regulations, the tasks of authorities and specific cyber threats.

6.2 Specific and common challenges

The previous section analysed the digitalisation and cybersecurity indicators to derive the relevant similarities and differences between the German and Israeli energy sectors. Based on this, the following section identifies and describes country-specific and cross-country challenges in the energy sectors resulting from political, regulatory and technical inhibitors as well as external conditions.

Germany: political barriers, regulatory complexity and missing standards

In Germany, the transition to a more digitalised energy sector is hindered by long approval processes for renewable energy projects, such as wind farms. This bureaucratic red tape slows the pace of grid expansion and complicates the integration of renewable energy sources. Additionally, Germany's stringent data privacy laws create barriers to widespread digital technology adoption. These laws restrict data collection and sharing, making it difficult to deploy smart meters (only 11 per cent coverage of electrical connections in Germany's energy sector) and optimise grid operations. The regulatory landscape itself adds complexity, with numerous updates since 2017, such as new market communication rules and redispatch regulations, making compliance a challenge for market participants and creates barriers for new entrants and smaller players.

[243] Workshop (2024)

This complexity is compounded by a lack of standardisation, which inhibits collaboration and technology integration across the energy sector, and by the absence of a unified data platform or data space, which makes Germany's energy market data exchange inefficient. Due to inconsistent standards, the granularity of smart meter data in Germany varies significantly, affecting its usefulness for data analytics.[244, 245, 246]

Germany: expanding and securing a decentralised grid with a high amount of renewables

Germany has achieved a comparable high installed capacity of renewables, including wind and solar, contributing to 53 per cent of its electricity generation. However, this reliance on variable energy sources demands sophisticated grid technologies to manage intermittency. At the same time, this leads to a sharp increase in converter-based energy generation, resulting in drastic changes in system operating principles, including system restoration in emergency cases. RES facilities need to contribute to the system stability by providing ancillary services and black start capabilities.[247]

Regulatory mandates require grid connection approvals within 56 days, but delays are common due to complex processes and grid congestion. Germany has achieved significant digitalisation in high-voltage grids but still struggles with medium- and low-voltage networks. Communication infrastructure in Germany relies on a mix of LTE, PLC and DSL, with rural areas facing connectivity issues.

The resulting highly decentralised energy infrastructure with its large number of interconnected systems drastically increases the attack surface especially for distribution systems (e.g., for APTs). In addition to this, there is an increasing threat against smart metering systems (e.g., by way of malware attacks).[248]

Germany: insufficient protection of OT systems

In the German energy sector, there are significant hurdles in implementing protective measures for OT systems due to legacy software and hardware components, very long update cycles and high-performance requirements of OT devices (e.g., time-critical processes). This is made even more difficult by the high prevalence of OT legacy systems, in which vulnerabilities are easily exploitable (e.g., by specially designed ICS malware) due to the lack of support from the manufacturers (EoS systems).[249, 250]

Israel: rigid grid management and limited energy diversity

The Israeli energy sector faces challenges primarily stemming from its reliance on a centralised grid managed by the IEC. This centralisation limits flexibility in integrating distributed energy resources (only 11 per cent renewable energy production), poses challenges for expanding a more decentralised energy system and limits third-party innovation opportunities. Although Israel benefits from abundant solar energy, the southern regions with high solar potential lie far away from the northern consumption areas. This and the lack of diversity in renewable energy sources complicate energy management and requires efficient storage and balancing mechanisms to ensure stability especially during non-peak solar periods. Israel's approval times are variable, averaging 67 days for positive responses but extending significantly for more complex cases depending on the geographic region. While Israel has made significant strides in digital grid oversight and smart meter penetration, achieving over 50 per cent coverage in some areas, gaps remain in fully modernising the energy infrastructure. Furthermore, while Israel's wired communication networks are robust, they require further development to ensure comprehensive and seamless connectivity across the entire grid.[251, 252, 253]

[244] Knüsel and Richard (2022)
[245] dena Future Energy Lab (2022)
[246] Workshop (2024)
[247] Bundesministerium für Wirtschaft und Klimaschutz (2023)
[248] Wagner and Chadenas (2022)
[249] Bundesamt für Sicherheit in der Informationstechnik (2022b)
[250] Bundesamt für Sicherheit in der Informationstechnik (2021)
[251] Mizrahi et al. (2024)
[252] Shakhak (2023)
[253] Ben Ari et al. (2022)

Israel: Grand strategies not publicly available and competing grid expansion plans

For the Israeli energy sector, ongoing efforts are needed to overcome challenges such as standardising data regulations and enhancing grid infrastructure to fully harness the benefits of digital advancements. This requires continued investment in grid infrastructure and regulatory support to fully integrate distributed energy resources and achieve national energy goals.[254, 255, 256, 257]

As referenced in Chapter 3, Israel's digital programme and cybersecurity strategy (only available in draft form) were both set up in 2017. After this, no updated strategic documents have been published by the government. In order to achieve the government's goals of increasing the share of renewable energy to 20 per cent by 2025 and to 30 per cent by 2030[258], different grid expansion plans are currently in progress at the MoE, Noga and PUA. Primarily due to the limited land resources in Israel, the construction of new RES facilities already poses the challenge of synchronising different authorities and ministries (e.g., PUA, land authority, MoE, Ministry of Agriculture).[259, 260]

The PUA grid expansion plan for 2025 is a draft document that foresees a doubling of RES installations to 9,000 MW as well as market participation for at least 80 per cent of these new facilities. In addition to the short time horizon, actual implementation of this plan is up in the air, especially since an energy market still has to be established. Noga's network development plan for 2030 has been approved by the PUA. This draft foresees a massive increase of solar rooftop facilities, transmission lines, underground cables and energy storage systems (between 400 and 500 MW in 2030). Lastly, the MoE is working on a multiyear plan for 2030, including RES installations up to 17,145 MW and the promotion of local authorities. These plans have not yet been finalised, are in part contradictory and the specific implementation remains unclear. Whereas the responsibility for meeting the renewable energy targets should rest with the MoE, the promotion of RES installations has necessarily lower priority for the corresponding authorities.

Israel: Operation Iron Swords and unclear legal basis for extensive INCD's powers

Israel's special geopolitical situation leads to an isolated energy infrastructure ('desert island') that is exposed to high risks from physical threats (e.g., EMP attacks) and cyber threats, with an ongoing trend towards destructive cyber-attacks (e.g., wiper-type ransomware). Operation Iron Swords, currently in progress, significantly intensifies this threat situation (2-3x increase in cyber incidents).[261, 262]

Despite a new cybersecurity bill from 2021, the INCD as the central cyber defence authority still has a vague legal basis defining its duties, functions and powers within the Israeli cybersecurity architecture. To maintain a high level of general security in the Israeli civilian cyberspace domain, privacy violations will necessarily occur, resulting in a lack of safeguards against invasive protective actions or other possible infringements on privacy by the INCD. Additionally, cybersecurity responsibilities are increasingly shifting away from private entities towards the INCD and sector-specific regulators compete in terms of the oversight functions they perform with the INCD.[263, 264]

Common digitalisation challenges: integration of renewables and smart meters, expansion of distribution grids and low digital maturity of SMEs

Germany and Israel share ambitious expansion goals for the transformation of their electricity grids requiring an increased integration of RESs and system flexibilities. Especially Israel faces significant challenges in expanding its electrical grid with new substations, high-voltage overhead power lines and energy storage systems. Still, long approval times for grid connections or expansion projects and an incomplete strategic framework stand in the way of efficient expansion of the distribution grids. Additional challenges remain for both countries regarding the expansion of smart meter systems to ensure standardised data access and granularity. SMEs in Israel and Germany face resource constraints that hinder the adoption of digital solutions and the investment in digital technologies including innovative business models. The digital maturity of these SMEs remains low, and inconsistent data

[254] Legal500 (2024)
[255] Arizona State University (2023)
[256] Tabansky (2021)
[257] International Trade Administration (2025)
[258] Surkes (2020b)
[259] Gov IL (2024j)
[260] Ben Ari et al. (2022)
[261] Mizrahi et al. (2024)
[262] Israel National Cyber Directorate (2023)
[263] Takaharu (2022)
[264] Housen-Couriel et al. (2021)

collection practices further complicate grid management.[265, 266, 267, 268]

Common cybersecurity challenges: lack of resources in SMEs, supply chain security and emergency training

Despite the large number of information sharing and supporting institutions (e.g., CSN in Germany or the ACD portal in Israel), German and Israeli SMEs have very limited financial and personnel resources to implement digital technologies or security controls efficiently. This lack of staff leads to greater use, and hence greater dependence, on external software and service providers (e.g., for maintenance work, data analytics or incident handling). Thus, additional entry points for cyber-attacks arise at remote access points or through the use of cloud-based services. To mitigate these security risks, both countries need to improve the supply chain security in their energy sectors, including with regards to manufacturers and vendors, with more strict and comprehensive security regulations. By providing and maintaining specialised technical solutions for all actors in the energy sector, manufacturers and vendors need to be more involved in cybersecurity architectures and are vital in the definition and implementation of common standards. The NIS2 directive already provides a basis for contractual security agreements between clients, providers and vendors as well as sets out increased requirements for vendors and manufacturers regarding risk management, incident handling and patch management.[269]

German and Israeli sector-specific CERTs lack funding and financial support. Corresponding emergency training is offered in Germany by private companies, whereas this is carried out by the national institutions (e.g., Nema and the IDF) in Israel as mandated by law. Still, more emergency training and simulations are necessary for relevant actors in the energy sector (e.g., system operators).[267, 266, 270, 271]

[265] Knüsel and Richard (2022)
[266] Workshop (2024)
[267] Schuster et al. (2024)
[268] Ben Ari et al. (2022)
[269] CI1 (2024)
[270] Schwarz (2023)
[271] Bundesamt für Sicherheit in der Informationstechnik (2023b)

7 Recommended actions and future projects

The energy sectors in Germany and Israel are facing significant digitalisation and cybersecurity challenges that hinder future improvements in the efficiency and security of energy infrastructures. As referenced in Chapter 6, these challenges range from regulatory issues such as long approval times to technical capabilities such as emergency response. This includes the systematic and efficient expansion of RES facilities made possible by short approval times for grid connections. This is complicated by Germany's high regulatory complexity and the lack of clear grid expansion plans in Israel. Other relevant challenges encompass the expansion of smart meter systems with standardised data access and granularity and the limited financial and personnel resources of SMEs. Additional needs arise with regards to implementing cybersecurity measures for OT systems, increased cybersecurity regulations for manufacturers and vendors as well as the improvement of emergency response capabilities of system operators. To cope with these challenges, several key areas for future innovations in the German and Israeli energy sectors have been derived. Examples include flexible market regulations for RES integration, common standards for smart meter systems, system flexibilities for improved grid balancing and shared frameworks to enhance OT and supply chain cybersecurity.

Using these findings, this chapter outlines recommended actions and potential future projects for the energy sectors in Germany and Israel. It highlights strategic initiatives that could enhance digital integration, improve cybersecurity and foster cross-country collaboration. Accordingly, Section 7.1 describes recommendations from a regulatory, process and technological perspective for the German and Israeli energy sector, addressing the digitalisation and cybersecurity challenges to guide policymakers and stakeholders. Building on this, Section 7.2 identifies common innovations and approaches considering the unique political and economic conditions in each country and outlines possible future collaborative projects that support long-term innovation and sustainability.

7.1 Regulatory, process and technological recommendations

Recommendations for the German energy sector

For the German energy sector, the recommendations address relevant digitalisation and cybersecurity aspects regarding the integration of RES, flexible energy markets and resilient system operation. This encompasses improved integration of RES facilities and system flexibilities for stable grid operation, simplified energy market processes, especially for the entry of new participants, increased resilience of system operation with a focus on restoration and emergency response capabilities, including cyber threats, and knowledge sharing regarding cyber threats targeting energy infrastructures. A more detailed description of the specific recommendations is provided below:

1. **Improve the contribution of RES to grid stability**: This includes the provision of ancillary services and the support of black start capabilities by RES facilities. This should be accompanied by further developments in technologies for system flexibility (e.g., demand side management, energy storage).[272, 273]
2. **Increase participation of market actors:** Greater involvement of industry associations such as the BDEW can greatly improve the design and evolution of energy market processes. Additionally, platforms like energy forums and expert forums should be utilised to incorporate practical industry feedback.[274, 275, 276]
3. **Simplify access to energy markets and the exchange of market data:** A streamlined process for integrating new market participants (especially start-ups), coupled with clear guidelines, is extremely important in order to foster innovation and business models in the energy market. Also, improved data access and more efficient communication between energy market actors using common standards should be facilitated (e.g., by providing open-source software and dataspaces for market communication processes).[275]

[272] Pfendler et al. (2022)
[273] Bundesministerium für Wirtschaft und Klimaschutz (2023)
[274] dena Future Energy Lab (2022)
[275] Knüsel and Richard (2022)
[276] Workshop

4. **Improve the observability of distribution systems:** Improved monitoring of distribution systems, including RES facilities and system flexibilities, is required to maintain stable system operation in view of future converter-based energy production.[273]
5. **Increase system restoration capabilities:** The communication and coordination between TSOs and DSOs should be strengthened, especially when it comes to the design and implementation of system restoration plans. Furthermore, new concepts should be investigated to build microgrids at the distribution level to support system restoration measures.[273]
6. **Foster exchange of information about cyber threats:** A knowledge base should be established that classifies cyber threats and describes possible mitigation measures for the energy sector (e.g., based on MITRE ATT&CK[277]).[278]
7. **Strengthen cyber defence capabilities:** This can be achieved by increasing emergency and security training for system operators and other relevant actors in the energy sector. In addition, sector-specific and interconnected security operation centres should be established to improve systemic cyber defence and enable proactive cybersecurity capabilities.
8. **Improve supply chain security**: This requires the implementation of security-by-design and security-by-default principles during production as well as the establishment of contractual agreements for support services (e.g., for incident and vulnerability handling) between manufacturers and clients. For this, manufacturers and vendors should maintain a comprehensive vulnerability management regime, including coordinated disclosure principles as well as effective patch development and testing.[279, 280]
9. **Increase funding for SMEs:** Investments in digitalisation and cybersecurity projects for SMEs should be given high priority to increase the digital maturity of SMES and to support industry innovations (e.g., blockchain-based energy trading or OT security measures).[276, 281]

Recommendations for the Israeli energy sector:

For the Israeli energy sector, the recommendations address relevant digitalisation and cybersecurity aspects regarding the expansion of RESs, a decentralised energy supply and emergency response to physical and cyber threats. This encompasses improvements in the integration of RES facilities (including agrivoltaic systems), the role of local authorities in facilitating the deployment of decentralised renewable energy solutions and the further development of emergency response capabilities. A more detailed description of the specific recommendations is provided below:

1. **Systematic expansion of renewable energies including agrivoltaics:** The further integration of renewable energy facilities using various energy sources in selected geographical regions is of great importance to reduce the dependence on certain energy sources (especially fossil power plants) and to make land use efficient. In particular, the future installation of agrivoltaic systems can provide significant support here. This should be complemented by energy storage and management solutions for improved grid integration.[282, 283, 284, 285]
2. **Increase participation of RES companies:** The establishment of a permanent forum for renewable energy entrepreneurs led by the MoE would improve the planning and implementation of future RES installations through direct feedback from the field.[284]
3. **Decentralisation of the energy supply with the involvement of local authorities:** Promoting local authorities as electricity suppliers would open the supply segment to competition and increase the efficiency of approval processes and regulation.[284]

[277] MITRE ATT&CK (2024e)
[278] ABSTAND FOR SCHWARZ (2023)
[279] Behre et al. (2022)
[280] Bundesamt für Sicherheit in der Informationstechnik (2018)
[281] Pfendler et al. (2022)
[282] Weinstock and Elran (2017)
[283] Mizrahi et al. (2024)
[284] Ben Ari et al. (2022)
[285] Gov IL (2024j)

4. **Promotion of energy complexes:** The fostering of pilots for energy complexes is highly important to enable the optimal utilisation of the energy resources while minimising the reliance on the electricity grid for importing and exporting energy.[284]
5. **Improve emergency response capabilities to handle physical and cyber threats:** This can be achieved by allocating financial resources to establish emergency response teams (e.g., to counter EMP attacks) and to implement a national emergency plan for the electricity grid.[282, 283]
6. **Improve supply chain security:** As part of international cooperation, improved regulations should be created for manufacturers and providers targeting more secure production processes (e.g., by means of security-by-design and security-by-default principles), regulated customer relationships and proactive vulnerability management.
7. **Increase funding for SMEs:** Investments in digitalisation and cybersecurity projects for SMEs should be given high priority to increase the digital maturity of SMES and to support industry innovations (e.g., blockchain-based energy trading or OT security measures).

7.2 Common innovations and possible future projects

The digitalisation of power grids is a critical element in the energy transition, and both Germany and Israel have adopted a range of innovative strategies tailored to their respective regulatory and infrastructural environments[286]. As referenced in Chapter 3, Germany's digital and cybersecurity strategies focus on the expanded use of smart measuring systems and flexible data sharing platforms as well as the protection of critical infrastructures and on ensuring financial support of SMEs and the security of supply chains. Israel is known as a start-up nation. The country pursues a digital programme which is heavily focusing on advancements in digital technologies to maintain its position as a leading technological innovator.

This section delves into the key advancements each country has embraced and discusses possible future collaborations to modernise grid operations, facilitate renewable energy integration and ensure system security, drawing on insights from workshops, expert forums and regulatory analysis.

Existing technology initiatives, innovation hubs and collaborations

Moreover, Germany's Connect+ platform facilitates efficient redispatch coordination, while the Gaia-X project aims to build a secure, cross-sector data infrastructure that enhances digital sovereignty and efficiency[287]. Given Israel's great potential in terms of solar energy, the country is investing in energy storage solutions and demand-side management to mitigate supply fluctuations. Innovations such as virtual power plants (VPPs) and microgrids are being explored to enhance grid resilience and ensure reliable energy supply during periods of low solar generation[288, 289].

Both Germany and Israel recognise the need for robust collaboration between the public and private sectors to foster technological advancements. Germany's energy sector benefits from the involvement of influential industry associations like the BDEW, which shape policy and encourage innovation. Israel, on the other hand, has established research and development hubs such as the ATP in Be'er-Sheba, fostering collaboration between academia, industry and government agencies[290]. These hubs are pivotal in advancing digital and cybersecurity solutions for energy infrastructure[291].

Apart from the German-Israeli Energy Partnership, several initiatives and collaborative ventures already exist between the two countries. These include:

- the *German-Israeli Chamber of Industry and Commerce's* efforts to assist Israeli companies in exploring and entering German markets[292];
- in November 2024 the BMDV and the Israeli Digital Agency initiated a *Digital Dialogue* to foster cooperation in the digital policy space between Germany and Israel in the fields of artificial intelligence, quantum computing and start-ups[293]; and

[286] Gov IL (2024j)
[287] Connect+ (2025)
[288] Abdelkader et al. (2024)
[289] Gloria et al. (2022)
[290] Knupper (2017)
[291] Strongin (2014)
[292] AHK (2025)
[293] BMDV (2025)

- a three-year German-Israeli research collaboration between ATHENE, a research centre of the Fraunhofer-Gesellschaft, sponsored by the Federal Ministry of Education and Research (BMBF) and the MoE to develop solutions for cybersecurity problems in the energy sector[294].

Key areas for future innovations and collaborative projects

The workshops and expert discussions underscore several promising areas for joint German-Israeli initiatives. Based on the digitalisation and cybersecurity challenges faced by the German and Israeli energy sector described in Section 6.2, the following key areas and possible projects for collaboration in future innovation fields have been identified:

Grid expansion and renewable energy integration: This encompasses collaborative efforts in sharing best practices for integrating distributed energy resources (e.g., solar power plants) using flexible market regulations while ensuring short grid connection approval times. This applies in particular to the distribution level and requires common regulations as well as the utilisation of appropriate grid expansion measures (e.g., energy storage). Here, Germany's experience in decentralised market operations could complement Israel's expertise in centralised grid management and support Israel in overcoming its strategic planning challenges.

Possible future projects

- Partnering in projects aiming to streamline grid connection of new RES and identification of viable solutions for circumventing capacity issues through novel approaches (e.g., automated digital processes for requests, combining volatile RESs with dynamic consumers)
- Facilitate knowledge transfer in ICT integration for distributed renewable energy resources (RESs), such as solar and wind power plants, to improve grid-level digitalisation and enable secure, efficient monitoring and control at the distribution level
- Joint academic and industrial research into agrivoltaic systems, leveraging digital technologies for precision monitoring, operational efficiency and secure data exchange, while fostering collaboration to exchange lessons learned in practical operations and develop scalable cybersecurity solutions for these innovative setups

Smart meter systems in liberalised energy markets: Here, the first smart metering initiatives have been already launched by both countries. Common benefits arise from Israel's centralised approach under the IEC to foster common standards for smart meter data rates and consumer access as well as Germany's experience gained in the strategically anchored smart meter rollout. Germany's focus on data spaces, such as Gaia-X, can improve the framework for identifying and establishing business cases by enabling secure and efficient data sharing and collaboration across stakeholders.

[294] ATHENE (2024)

Possible future projects

- Working or expert groups focused on common standards for smart meter data rates and data access
- Joint research involving academia, industrial associations and start-ups to develop efficient energy market processes and integrate approaches for new market participants
- Pilot projects to identify and demonstrate business cases using smart meter data by integrating blockchain technology or data spaces (e.g., Gaia-X)
- Pilot projects to empower consumers through personalised energy usage insights and cost-saving measures

Energy storages and other system flexibilities: This includes joint research on the applicability of different system flexibility technologies to facilitate the integration of RESs and to improve grid balancing. This research could greatly benefit from Germany's experience using energy storage systems (e.g. home battery systems or large scale battery storage systems for anciallary services), demand-side management, virtual power plants and microgrids, in particular to maintain stable system operation (e.g. home battery systems or large scale battery storage systems for anciallary services). Existing smart metering infrastructures in both countries could support initiatives for future collaborations. These initiatives should address and support SMEs in order for them to make better use of digital technologies and to identify new business models.

Possible future projects

- Pilot projects for energy storage, virtual power plants or microgrids, focusing on advanced digital tools for handling large-scale data and creating resilient processes for grid support (e.g., ancillary services and black start capabilities) while ensuring robust cybersecurity measures to protect these systems from vulnerabilities

Protection of OT systems and SMEs: Innovative developments for efficient and scalable security solutions are necessary to protect (legacy) OT systems. This could greatly benefit from Israel's successful OT security practices and experiences from the last decade. Insights from past cyber incidents, such as cyber-attacks on European wind farms or sector-specific incidents during Operation Iron Swords in Israel, can provide further insights for a more in-depth exchange of information. In particular, the support of SMEs in terms of personnel and financial resources should be addressed to better meet current and future regulatory requirements including the implementation of sufficient security controls.

Possible future projects

- Platform to share experience and to build up a knowledge base regarding the classification and handling of cyber incidents in the energy sector
- Pilot projects bringing together research institutes, tech companies and SMEs to develop more efficient cybersecurity measures to protect OT systems and devices
- Joint research between academia and industry to improve and standardise service-oriented monitoring, maintenance and security solutions for SMEs in the energy sector
- Working or expert groups made up of governmental institutions and industry associations to establish new funding possibilities for SMEs in raising digital maturity and cyber protection

Supply chain security for manufacturers and vendors: The establishment of shared security frameworks based on common research (e.g., the ATHENE partnership) and common standards is highly relevant to fostering cybersecurity collaborations between the two countries. In particular, international initiatives are necessary to adopt upgraded cybersecurity regulations and processes for large manufacturers and vendors, thus increasing the supply chain security in the energy sector. The consistent implementation of security-by-design and security-by-default principles within production can greatly minimise potential cyber risks arising from supply chain attacks.

Possible future projects

- International working groups to develop shared cybersecurity frameworks and standards for manufacturers and providers based on harmonised and efficient regulations (e.g., NIS2 Directive[1], EU grid codes[1], EU Cyber Resilience Act[1])
- International initiative to establish a culture fostering a holistic cybersecurity landscape in the energy sector, including industry stakeholders, manufacturers and vendors
- Pilot projects incorporating solar and wind power plant manufacturers for cost-efficient and secure production processes (e.g., using security-by-design and security-by-default principles), in the process identifying potential business values (e.g., security branding)
- Joint research and collaboration to establish exchange platforms, including secure and efficient communication options between manufacturers and clients to improve communication regarding cyber risks and the handling of hardware and software vulnerabilities

Emergency training in the energy sector: Carrying out and improving the quality of emergency training are highly important in both countries to better cope with cyber incidents in the energy sector. Corresponding cooperations, including the exchange of experience and identifying best practices, could benefit from the existing Israeli emergency response activities to cope with large-scale cyber-attacks (e.g., emergency training for system operators conducted by the MoE, NEMA and the IDF).

Possible future projects

- Working group including industry experts and governmental institutions to improve emergency training for system operators, increase financial support for CERTs and establish a regulatory framework at a national scale
- Share experience and best practices to establish and maintain sector-specific and interconnected security operation centres for different actors in the energy sector
- Joint research to improve the emergency response and system restoration capabilities when coping with extreme events at a national scale, including natural disasters, military attacks or cyber incidents

AI business cases in digitalised energy grids: Artificial intelligence (AI) offers the potential for high-value business cases in the energy sector, such as optimising grid performance or forecast energy demand. For this, Germany's projects in AI-based grid management and Israel's cybersecurity capabilities build a fertile ground for collaboration. This can be further enhanced by Israel's start-up approach fostering tech companies, especially in the cyber space (e.g., ATP in Be'er-Sheba or CyberSpark). AI applications require a high level of digital maturity at the companies. SMEs should be supported to improve their data collection and management practices.

Possible future projects

- Joint research regarding the potential of AI technology to improve the efficiency and reliability of system restoration and emergency response applications
- Big data platform for AI companies and start-ups to leverage smart meter data to explore AI-driven solutions (e.g., demand response, energy forecasting)

8 Conclusion and summary

The energy sector is experiencing a major transformation through the integration of renewable sources, leveraging system flexibilities such as energy storage, electric vehicles and demand response mechanisms. Digital technologies are crucial for developing flexible and decentralised energy systems that provide an efficient, reliable and sustainable energy supply. However, this transformation also introduces significant cybersecurity risks, particularly for OT systems that use legacy or proprietary technology. The transition from centralised fossil fuel power plants to distributed renewable energy sources necessitates prioritising cybersecurity to protect critical infrastructure and ensure a safe and resilient energy system. Strengthening energy infrastructures has become increasingly important for both the German and Israeli governments. Both countries have historically pursued this approach and are now shifting towards a more dynamic infrastructure to accommodate large amounts of energy production from renewable energy sources in lower-voltage grids.

The German energy sector: decentralised infrastructure and the energy transition

The German energy sector is undergoing a significant transformation, focusing on a digital strategy that emphasises the implementation of smart measuring systems and the development of data spaces or platforms to enhance efficiency and integration. Concurrently, the cybersecurity agenda prioritises the protection of critical infrastructures, with financial support directed particularly at SMEs, to ensure the security of supply chains. The German energy transition is leading to a highly decentralised energy system, characterised by a substantial shift towards renewable energy sources, with about 60 per cent of electricity production coming from renewables (primarily wind and solar) in 2024. This shift has resulted in a large number of local energy providers and renewable energy installations, predominantly owned by municipalities, cooperatives and private companies. However, the decentralised nature and reliance on digital systems pose a high risk for cyber-attacks, particularly targeting the distribution system and smart metering systems. Overall, Germany is navigating the challenges of its energy transition while prioritising digital innovation and cybersecurity.

The Israeli energy sector: centralised 'energy island' and proactive cyber defence

The Israeli energy sector is positioned within a landscape of innovation and security challenges. Known as the start-up nation, Israel leverages advances in digital technology to maintain its role as a leading technological innovator, supported by high levels of funding and investment in start-ups and tech companies. The energy infrastructure remains highly centralised, although there has been a noticeable increase in private ownership. Energy production in Israel comprises both conventional and renewable sources, with solar being the primary source of renewable energy. However, grid connection approval times are long and vary significantly based on project complexity. Due to limited connections to neighbouring countries, Israel functions as an energy island, impacting its energy independence and security. Cybersecurity is of the utmost priority for the country, guided by a proactive cyber defence strategy developed through strong military and civilian cooperation. This is crucial as Israel faces numerous physical and cyber-attacks, especially since Operation Iron Swords, with an increasing shift towards destructive attacks and a high level of risk from EMP threats. This evolving threat landscape underscores the importance of robust cybersecurity measures and infrastructure resilience.

Similarities and common challenges: from integration of renewables to OT cybersecurity

Germany and Israel are both advancing their energy sectors to achieve a carbon-free energy supply with a strong focus on solar energy technologies. As part of their efforts to diversify and decentralise electricity production, both countries are integrating DERs and are upgrading their grid management systems by investing in smart meters to enable real-time monitoring, automation and efficient communication networks. Regarding cybersecurity, Germany and Israel have established central authorities to oversee cybersecurity efforts: the BSI in Germany and the INCD in Israel. Ransomware and supply chain attacks have been identified as common cyber threats in both sectors, along with systemic weaknesses such as the inadequate protection of OT devices, vulnerabilities in remote access points and insufficient regulation of manufacturers and providers.

Both countries have ambitious goals to transform their energy systems towards renewable energies. In particular, the long approval times for grid connections pose significant delays, impeding the integration of new RES facilities and system flexibilities. The expansion of smart meter systems requires standardised data access and granularity, while at the same time interoperability and data privacy issues must also be addressed. Furthermore, SMEs in both countries often lack the resources to invest in digital technologies and innovative business models. They struggle with the financial and resource demands of compliance and adapting to rapid technological changes, which can stymie the overall digitalisation progress in the energy sector.

From a cybersecurity perspective, one significant hurdle is the implementation of protective cybersecurity measures for OT systems especially for small production units, which are crucial for managing energy infrastructure. Additionally, there is an increasing need to establish appropriate regulations for software and hardware manufacturers to ensure they meet cybersecurity standards. SMEs face particular difficulties due to their limited financial and personnel resources, making it challenging to implement robust security controls efficiently. Moreover, both countries face a major threat from supply chain attacks, where adversaries target vulnerabilities in the supply chain to compromise systems. Also, there is a need for more training and simulations for relevant actors in the energy sector. Such initiatives would enhance the preparedness and response capabilities of personnel, helping to mitigate the risks associated with potential cyber incidents.

Key areas for common innovation: integration of renewables, smart metering, OT cybersecurity, supply chains, cyber response

To address the challenges in the German and Israeli energy sectors, a number of innovation areas and associated future projects have been identified for possible areas for future collaboration.

Renewable energy integration: Improvements in the integration of distributed energy resources (e.g., solar power plants) are necessary in both countries and require flexible market regulations and short grid connection approval times. Innovations in this field should focus on the applicability of different system flexibility technologies to facilitate the integration of RESs and to improve grid balancing. Future projects could include:

- the share of expertise and best practices in the integration of RES facilities;
- pilot projects for energy storage, virtual power plants or microgrids; and
- academic and industrial research for agrivoltaic systems.

Smart metering and energy markets: Common standards for smart meter data rates and consumer access are relevant for further innovations in this area. This goes hand in hand with the development of efficient energy market processes and the simple, non-bureaucratic integration of new energy market participants. Possible future projects might include:

- expert groups for common standardisation of smart meter data rates and data access;
- pilot projects to identify and demonstrate business cases using smart meter data (e.g., Gaia-X); and
- a big data platform for AI companies and start-ups to leverage smart meter data.

OT cybersecurity: In both countries, SMEs lack staff and financial resources to meet current and future regulatory requirements. An adequate level of protection for legacy OT systems is also an open challenge. Possible future projects might include:

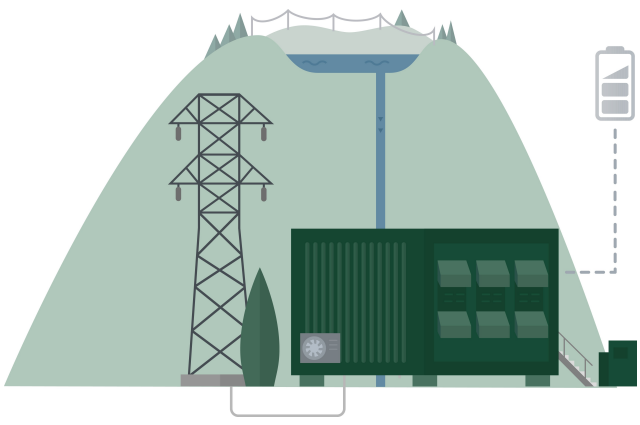
- building up a knowledge base regarding the classification and handling of cyber incidents in the energy sector;
- bringing together research institutes, tech companies and SMEs to develop more efficient cybersecurity measures; and
- joint research to improve and standardise service-oriented monitoring, maintenance and security solutions for SMEs.

Supply chain security and manufacturers: The development of shared frameworks based on common standards is highly relevant to foster cybersecurity collaborations. Innovations in this field should improve cybersecurity regulations especially for manufacturers and providers in the OT domain. Possible future projects might include:

- International initiatives to foster a holistic cybersecurity landscape;
- International working groups to develop shared cybersecurity frameworks and standards; and
- Collaboration on efficient platforms for manufacturers and clients to exchange information.

System restoration and emergency response: The handling of emergencies (e.g., large-scale cyber-attacks) and the efficient restoration of relevant systems represent an important area for future innovation in the energy sector in both countries. The exchange of experience and the identification of best practices can be highly beneficial for both countries. Possible future projects might include:

- sharing experience and best practices to establish and maintain sector-specific and interconnected security operation centres;
- joint research to upgrade emergency response and system restoration capabilities when coping with extreme events at a national scale, including natural disasters, military attacks or cyber incidents; and
- joint research regarding the utilisation of AI technology to improve the efficiency and reliability of system restoration and emergency response applications.
- Collaboration and share of best-practices for the improvement of incident response and emergency trainings.



9 List of figures

10 List of tables

11 Bibliography

Abdelkader, S., Amissah, J., & Abdel-Rahim, O. (2024). Virtual power plants: an in-depth analysis of their advancements and importance as crucial players in modern power systems. ***Energy, Sustainability and Society***, ***14***(1). https://doi.org/10.1186/s13705-024-00483-y

ACD/Labs. (2024). ***Register for a Customer Portal Account*** | *ACD/Labs*.

Aggregators. (2019). ***AGGREGATORS: INNOVATION LANDSCAPE BRIEF***. (2019).

AHK. (2025). *The German-Israeli Chamber of Industry & Commerce.* https://israel.ahk.de/en/about-us/the-german-israeli-chamber-of-industry-&-commerce

Amprion. (2025). ***Connect +: Datenaustausch für Redispatch 2.0 startet.*** https://www.amprion.net/Presse/Presse-Detailseite_33408.html

Ardagna, C., Corbiaux, S., Van Impe, K., & Ostadal, R. (2023). ***ENISA THREAT LANDSCAPE 2023: July 2022 to June 2023.***

Arghire, I. (2022). Conti Ransomware Gang Claims Cyberattack on Wind Turbine Giant Nordex. ***SecurityWeek.*** https://www.securityweek.com/conti-ransomware-gang-claims-cyberattack-wind-turbine-giant-nordex/

Arizona State University. (2023). ***ASU Hosts U.S.-Israel Workshop on Cybersecurity in the Energy Sector.*** https://fullcircle.asu.edu/fulton-schools/asu-hosts-u-s-israel-energy-cybersecurity-workshop/

Assante, M. J., & Lee, R. M. (2015). ***The Industrial Control System Cyber Kill Chain.***

ATHENE. (2024). ***ATHENE launches German-Israeli research cooperation on cyber security in the energy sector.*** https://www.athene-center.de/en/news/news/athene-launches-german-israeli-research-cooperatio-1632

Avri Eitan (2023). How are public utilities responding to electricity market restructuring and the energy transition? Lessons from Israel. ***Utilities Policy***, ***82***, 101562. https://doi.org/10.1016/j.jup.2023.101562

Bayer, E. (2015). ***Report on the German power system.*** Version 1.2.

BDEW Bundesverband der Energie- und Wasserwirtschaft (2023b). ***Anlagen oder Systeme zur Steuerung und Bündelung elektrischer Leistung (BS3 Aggregatoren): Nach § 8a Abs. 2 BSI-Gesetz.*** Version: 1.2.

BDEW Bundesverband der Energie- und Wasserwirtschaft. (2023a). ***German Power and Gas Grid 2023.*** https://www.bdew.de/media/documents/20230609_Deutsches_Strom_und_Gasnetz_Ver%C3%B6ffentlichung_003.pdf

Behre, C., Daniel, C., Fengler, D., Greven, S., Jünger, A., Sachgau, C., Schlüter, P., Schmidt, L., Töbich, P., & Wienand, T. (2022). ***Empfehlungen zu Entwicklung und Bereitstellung von in Kritischen Infrastrukturen eingesetzten Produkten.*** Erstellt durch Themenarbeitskreis Lieferanten/Hersteller des UP KRITIS. www.bsi.bund.de/dok/980540

Ben Ari, H., Dolev, S., Shalom, J., & Kaner, N. (2022). ***Road map for renewable energies in 2030.*** https://www.gov.il/BlobFolder/news/re_290522/he/roadmap_reference_2030

BMDV. (2025). ***Deutschland und Israel starten Digitaldialog.*** https://bmdv.bund.de/SharedDocs/DE/Pressemitteilungen/2024/104-digitaldialog-deu-isr.html

Böswetter, M., & Richard, P. (2021). ***Digitale Markommunikation für das Energiesystem der Zukunft.*** Gutachten.

Böswetter, M., Bader, L., Henze, M., Rademacher, M., van der Velde, D., Sen, Ö., & Andres, M. (2021). ***EnerCrypt: Cyber Innovations for the Secure Energy System of the Future.***

Brook, C. (2016). Israeli Electric Authority Hit by 'Severe Cyber-Attack,' Likely Ransomware. ***Threatpost.*** https://threatpost.com/israeli-electric-authority-hit-by-severe-cyber-attack-likely-ransomware/116036/

Buckley, J. & Connor, S. (2023). ***Israel-Hamas conflict to heighten cyber espionage and disruptive cyber threats.*** https://www.controlrisks.com/our-thinking/insights/israel-hamas-conflict-to-heighten-cyber-espionage-and-disruptive-cyber-threats

Bundesamt für Sicherheit in der Informationstechnik. (2018). ***Handhabung von Schwachstellen: Empfehlungen für Hersteller.*** EMPFEHLUNG: IT-HERSTELLER. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Allgemeine-Empfehlungen/Empfehlungen-fuer-Hersteller-und-Integratoren/empfehlungen-fuer-hersteller-und-integratoren_node.html

Bundesamt für Sicherheit in der Informationstechnik. (2021). ***CERT-Bund.*** https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html

Bundesamt für Sicherheit in der Informationstechnik. (2022a). ***UP KRITIS.*** https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/UP-KRITIS/up-kritis_node.html

Bundesamt für Sicherheit in der Informationstechnik. (2022b). ***Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen.*** BSI-CS 005. https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.html?nn=128730

Bundesamt für Sicherheit in der Informationstechnik. (2023a). ***Auftrag.*** https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html

Bundesamt für Sicherheit in der Informationstechnik. (2023b). ***Die Lage der IT-Sicherheit in Deutschland 2023.*** BSI-LB23/512. Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik. (2024). ***ICS-Security-Kompendium.*** Version 2.0.0.

Bundesministerium des Innern und für Heimat. (2021). ***Cybersicherheitsstrategie für Deutschland 2021.***

Bundesministerium des Innern und für Heimat. (2022). ***Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat: Ziele und Maßnahmen für die 20. Legislaturperiode.*** BMI22011.

Bundesministerium für Wirtschaft und Klimaschutz. (2023). ***Roadmap Systemstabilität: Fahrplan zur Erreichung eines sicheren und robusten Betriebs des zukünftigen Stromversorgungssystems mit 100 % erneuerbaren Energien.*** https://www.bmwk.de/Redaktion/DE/Publikationen/Energie/20231204-roadmap-systemstabilitaet.html

Bundesnetzagentur. (2023). ***Monitoringbericht 2023: Marktbeobachtung.*** https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Monitoringberichte/start.html

Bundesnetzagentur. (2024). ***Aufgaben und Struktur.*** https://www.bundesnetzagentur.de/DE/Allgemeines/DieBundesnetzagentur/AufgabenStruktur/start.html

Bundesnetzagentur. (2025a). ***Beschlusskammern - Messstellenbetriebsgesetz (MsbG).*** https://www.bundesnetzagentur.de/DE/Beschlusskammern/BK08/BK8_09_MsbG/BK8_MsbG_Basepage.html

Bundesnetzagentur. (2025b). ***Core energy market data register.*** https://www.bundesnetzagentur.de/EN/Areas/Energy/CoreEnergyMarketDataRegister/start.htm

Bundesnetzagentur. (2025c). ***Redispatch.*** https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/Netzengpassmanagement/Engpassmanagement/Redispatch/start.html

Bundesnetzagentur. (2025d). ***Press - Confirmation of electricity grid reserve capacity requirements.*** (24 January 2025). https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2024/20240430_Netzreserve_Pb.html

Bundesnetzagentur. (2025e). ***IT-Sicherheit für Energieanlagen.*** https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/IT_Sicherheit/Anlagenbetreiber/start.html

Bundesnetzagentur. (2025f). ***Homepage - IT-Sicherheitskatalog für Strom- und Gasnetze.*** (24 January 2025). https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/IT_Sicherheit/Netzbetreiber/artikel.html

Bundesnetzagentur. (2025g). ***Grid connection.*** https://www.bundesnetzagentur.de/EN/Areas/Energy/NetworkAccess_Metering/GridConnection/start.html

Bundesregierung. (2024). ***Digitalstrategie: Digitaler Fortschritt | Die Bundesregierung informiert.*** https://www.bundesregierung.de/breg-de/themen/digitalisierung/digitalstrategie-2072884

Bundesregierung. (2025). ***28. Weltklimakonferenz in Dubai | Die Bundesregierung informiert.*** https://www.bundesregierung.de/breg-de/aktuelles/cop-28-2246298

Central, S. N. (2024). ***Powering the Future: The Role of Israeli Innovation in Advancing Energy Tech - Startup Nation Central.*** https://startupnationcentral.org/hub/blog/powering-the-future-the-role-of-israeli-innovation-in-advancing-energy-tech/

CI1. (2024). CI1, B. M.I. ***Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung.***

Clean Energy Wire. (2022). ***Germany's 2022 renewables and efficiency reforms.*** https://www.cleanenergywire.org/factsheets/germanys-2022-renewables-and-energy-reforms

Clou, S. (2023). From peak demand to lower prices: The benefits of dynamic pricing enabled by smart meters. ***Smart Energy International.*** https://www.smart-energy.com/industry-sectors/smart-meters/from-peak-demand-to-lower-prices-the-benefits-of-dynamic-pricing-enabled-by-smart-meters/

Cohen, M. S., Freilich, C. D., & Siboni, G. (2015). Israel and Cyberspace: Unique Threat and Response. ***International Studies Perspectives***, ekv023. https://doi.org/10.1093/isp/ekv023

Cohen, S. (2019). Iranian Cyber Capabilities Assessing the Threat to Israeli Financial and Security Interests. ***Cyber, Intelligence, and Security, Volume 3, No. 1.***

Connect+. (2025). ***Presse – Connect+.*** https://netz-connectplus.de/home/presse/

Courier Mail. (2024). ***High voltage: BlackRock backs battery roll out.*** https://www.couriermail.com.au/subscribe/news/1/?sourceCode=CMWEB_WRE170_a&dest=https%3A%2F%2Fwww.couriermail.com.au%2Fbusiness%2Fqld-business-weekly%2Fhigh-voltage-blackstone-backs-battery-roll-out%2Fnews-story%2F33cfc1a69af7220d6e42240efb580947&memtype=anonymous&mode=premium&v21=GROUPA-Segment-2-NOSCORE

Csanyi, E. (2017). The Structure of Electric Power Systems (Generation, Distribution and Transmission Of Energy). ***Electrical Engineering Portal.*** https://electrical-engineering-portal.com/electric-power-systems

CYBERsicher. (2024). ***Cybersicherheit für den Mittelstand CYBERsicher.*** https://transferstelle-cybersicherheit.de/

Cybertech (2025). ***Israel Deploying Cyber Shield for 'HazMat' Industry | Cybertech Global Tel Aviv.*** https://www.cybertechisrael.com/node/1275

David, B. (2022). ***Wind Turbine Giant Nordex Hit By Cyber-Attack.*** Infosecurity Magazine. https://www.infosecurity-magazine.com/news/wind-turbine-nordex-cyber-attack/.

dena Future Energy Lab. (2022). ***dena-GUTACHTEN: Digitale Marktkommunikation für das Energiesystem der Zukunft - dena Future Energy Lab.*** https://future-energy-lab.de/news/gutachten-digitale-marktkommunikation/

dena Future Energy Lab. (2024). ***Branchenplattform Cybersicherheit - dena Future Energy Lab.*** https://future-energy-lab.de/projects/branchenplattform-cybersicherheit/

dena Future Energy Lab. (2025). ***Startseite - dena Future Energy Lab.*** https://future-energy-lab.de/

Desk, N. (2024). ***EDF Renewables pick mPrest as DERMS provider for advanced grid-aware system.*** https://www.iotinsider.com/industries/industrial/edf-renewables-pick-mprest-as-derms-provider-for-advanced-grid-aware-system/

Devolo AG. (2019). ***PLC Technology for Rollout: White Paper.*** https://www.devolo.de/fileadmin/Web-Content/DE/Contentseiten/Smart_Grid/PLC-Technologie/DE/Whitepaper_PLC-fuer-Rollout_0119_DE.pdf

Dhlamini, T., & Mawela, T. (2022). Critical Success Factors for Information Technology and Operational Technology Convergence Within the Energy Sector. In A. Abraham (Ed.), ***Lecture Notes in Networks and Systems Ser: v.419. Innovations in Bio-Inspired Computing and Applications: Proceedings of the 12th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2021) Held During December 16-18 2021*** (Vol. 419, pp. 425–434). Springer International Publishing AG. https://doi.org/10.1007/978-3-030-96299-9_41

Digitalstrategie Deutschland. (2024). ***Digitalstrategie: Gemeinsam digitale Werte schöpfen.*** https://digitalstrategie-deutschland.de/

DKE. (2022). ***Gaia-X für die Energiewirtschaft.*** https://www.dke.de/de/arbeitsfelder/energy/gaia-x-fuer-die-energiewirtschaft

E3P. (2025). ***Demand Response status in Member States: Mapping through real case experiences | E3P.*** https://e3p.jrc.ec.europa.eu/articles/demand-response-status-member-states-mapping-through-real-case-experiences

Elmas, D. S. (2024). High demand for switching electricity suppliers. ***Globes.*** https://en.globes.co.il/en/article-High-demand-for-switching-electricity-suppliers-1001486015

Enerdata. (2024). ***Israel unveils new reform to open electricity market to private providers.*** https://www.enerdata.net/publications/daily-energy-news/israel-unveils-new-reform-open-electricity-market-private-providers.html

Energy Gov. (2025). ***Operational Technology Cybersecurity for Energy Systems.*** https://www.energy.gov/femp/operational-technology-cybersecurity-energy-systems

Energy Storage Journal. (2025). ***Israel green light for first national ESS plan.*** Energy Storage Journal. https://www.energystoragejournal.com/israel-green-light-for-first-national-ess-plan/

Energy. (2025). ***Electricity network codes and guidelines.*** https://energy.ec.europa.eu/topics/markets-and-consumers/wholesale-energy-market/electricity-network-codes-and-guidelines_en

ENTSO-E. (2015a). ***Towards smarter grids: Developing TSO and DSO roles and interactions for the benefit of consumers.*** Position Paper. https://www.entsoe.eu/2015/03/04/towards_smarter_grids_entso-e_position_paper_on_developing_tso_and_dso_roles_for_the_benefit_of_consumers/

ENTSO-E. (2015b). ***General Guidelines for Reinforcing the cooperation between TSOs And DSOs.*** https://www.entsoe.eu/2015/11/09/general_guidelines_for_reinforcing_the_cooperation_between_tsos_and_dsos/

ENTSO-E. (2024) ***ENTSO-E publishes the Market Report 2024, the Balancing Report 2024 and the Electricity Balancing (EB) Cost Report 2024.*** https://www.entsoe.eu/news/2024/06/28/entso-e-publishes-the-market-report-2024-the-balancing-report-2024-and-the-electricity-balancing-eb-cost-report-2024/

ENTSO-E. (2025a). ***Power Regions.*** https://www.entsoe.eu/regions/

ENTSO-E. (2025b). ***Common Information Model (CIM) for Energy Markets.*** https://www.entsoe.eu/digital/common-information-model/cim-for-energy-markets/

Euractiv. (2023). ***Germany outlines plan to expand, digitalise power grids - Euractiv.*** https://www.euractiv.com/section/electricity/news/germany-outlines-plan-to-expand-digitalise-power-grids/

Federal Statistical Office. (2023). ***Gross electricity production in 2022: 44% came from renewable energy sources.*** https://www.destatis.de/EN/Themes/Economic-Sectors-Enterprises/Energy/Production/gross-electricity-production.html

FfE. (2023). ***Der Smart Meter Rollout in Deutschland und Europa - FfE.*** https://www.ffe.de/veroeffentlichungen/smart-meter-rollout-in-deutschland-und-europa/

Fischer, L., Uslar, M., Morrill, D., Döring, M., & Haesen, E. (2018). ***Study on the Evaluation of Risks of Cyber-Incidents and on Costs of Preventing Cyber-Incidents in the Energy Sector.*** final Report.

FKIE, F. (2025a). ***Havex RAT (Malware Family).*** https://malpedia.caad.fkie.fraunhofer.de/details/win.havex_rat

FKIE, F. (2025b). ***Industroyer (Malware Family).*** https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer

FKIE, F. (2025c). ***RedLine Stealer (Malware Family).*** https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer

FKIE, F. (2025d). ***Triton (Malware Family).*** https://malpedia.caad.fkie.fraunhofer.de/details/win.triton

Fortinet. (2025). ***What is the CIA Triad and Why is it important? | Fortinet.*** https://www.fortinet.com/resources/cyberglossary/cia-triad

Fraunhofer Institute for Solar Energy Systems ISE. (2025a). *Net Electricity Generation in Germany in 2022: Significant Increase in Generation from Wind and PV - Fraunhofer ISE.* https://www.ise.fraunhofer.de/en/press-media/press-releases/2023/net-electricity-generation-in-germany-in-2022-significant-increase-in-generation-from-wind-and-pv.html

Fraunhofer Institute for Solar Energy Systems ISE. (2025b). ***Public Electricity Generation 2023: Renewable Energies Cover the Majority of German Electricity Consumption for the First Time - Fraunhofer ISE.*** https://www.ise.fraunhofer.de/en/press-media/press-releases/2024/public-electricity-generation-2023-renewable-energies-cover-the-majority-of-german-electricity-consumption-for-the-first-time.html

Fraunhofer Institute for Solar Energy Systems ISE. (2025c). ***Smart Metering and Grid Control - Fraunhofer ISE.*** https://www.ise.fraunhofer.de/en/business-areas/power-electronics-and-grids/smart-metering-and-grid-control.html

Frei, J. (2020). ***Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations.*** https://doi.org/10.3929/ETHZ-B-000438397

Freilich, C. D. (2018). ***Israeli national security: A new strategy for an era of change.*** Oxford University Press. https://doi.org/10.1093/oso/9780190602932.001.0001

Ganot, S. (2022). ***Israeli Renewable Energy Power Facilities Increase by Almost 50% in 2021 - The Media Line.*** https://themedialine.org/mideast-daily-news/israeli-renewable-energy-power-facilities-increase-by-almost-50-in-2021/

Ganot, S. (2024). ***Israel, Germany Partner To Enhance Cybersecurity in Energy Sector - The Media Line.*** https://themedialine.org/mideast-daily-news/israel-germany-partner-to-enhance-cybersecurity-in-energy-sector/

Gav-Yam Negev. (2024). ***Home - Gav-Yam Negev.*** https://www.gavyam-negev.co.il/en/

Global Legal Group. (2025). ***Renewable Energy Laws and Regulations Report 2025 Israel.*** Global Legal Group. https://iclg.com/practice-areas/renewable-energy-laws-and-regulations/israel

Globes. (2022). ***IEC to install one million smart meters.*** https://en.globes.co.il/en/article-IEC-to-install-one-million-smart-meters-1001409530

Gloria, L. L., Righetto, S. B., Oliveira, D. B. S. de, Martins, M. A. I., Kraemer, R. A. S., & Ludwig, M. A. (2022). Microgrids and Virtual Power Plants: Integration Possibilities. In ***2022 2nd Asian Conference on Innovation in Technology (ASIANCON)*** (pp. 1–4). IEEE. https://doi.org/10.1109/ASIANCON55314.2022.9909430

Gov IL. (2024a). ***The submarine power cable is Under Way!*** https://www.gov.il/en/pages/news-040723

Gov IL. (2024b). ***About Ministry of Energy Ministry of Energy and Infrastructure.*** (21 July 2024). https://www.gov.il/en/pages/about_ministry_of_energy

Gov IL. (2024c). ***The Electricity Authority.*** https://www.gov.il/en/departments/the_electricity_authority/govil-landing-page

Gov IL. (2024d). ***Promotion of Renewable Energy in the Israeli Energy Sector.*** https://www.gov.il/en/pages/renewable_energy

Gov IL. (2024e). ***Yuval system - introduction to the system from the National Cyber System.*** https://www.gov.il/he/pages/yuvalrisk

Gov IL. (2024f). ***About Israel National Cyber Directorate Israel National Cyber Directorate.*** (21 July 2024). https://www.gov.il/en/pages/newabout

Gov IL. (2024g). ***The operating principles of the National CERT from the National Cyber System.*** https://www.gov.il/he/pages/certpri

GOV IL. (2024h). ***Department of Emergency, Security, Information, and Cyber.*** https://www.gov.il/en/departments/units/energy_security

Gov IL. (2024i). ***About ICNL - ICS Cybersecurity National Lab ICNL - ICS Cybersecurity National Lab.*** (21 July 2024). https://www.gov.il/en/pages/about_icnl

Gov IL. (2024j). ***Cybernet Israel National Cyber Directorate.*** (21 July 2024). https://www.gov.il/en/pages/cybernet

Gov IL. (2024k). ***Renewable Energies in Israel: Compliance status on the map: The ways to 2030***, Economy Committee of the Knesset. https://www.gov.il/BlobFolder/reports/re-nov-2024/he/re-nov-2024

Grotz, F., & Schroeder, W. (2023). The Political System of Germany: Analytical and Historical Foundations. In F. Grotz (Ed.), ***New Perspectives in German Political Studies. The Political System of Germany*** (1st ed., pp. 1–31). Springer International Publishing AG. https://doi.org/10.1007/978-3-031-32480-2_1

Gutglik, I., Zachar, Y., & Levy, A. (2023). ***Report on the State of the Electricity Sector: Summary of 2022 and Trends in 2023.***

Housen-Couriel, D. & Mimran, T. & Shany, Y. (2021). ***Israel's Version of Moving Fast and Breaking Things: The New Cybersecurity Bill.*** https://www.lawfaremedia.org/article/israels-version-moving-fast-and-breaking-things-new-cybersecurity-bill

Housen-Couriel, D. (2017). ***National Cyber Security Organization: ISRAEL.***

IBM. (2025). ***What Are Smart Meters?*** | *IBM.* https://www.ibm.com/think/topics/smart-meter

IEA. (2025a). ***Countries can transform the global energy sector by fully implementing the 2030 goals they agreed at COP28 - News - IEA.*** https://www.iea.org/news/countries-can-transform-the-global-energy-sector-by-fully-implementing-the-2030-goals-they-agreed-at-cop28

IEA. (2025b). ***Germany - Countries & Regions - IEA.*** https://www.iea.org/countries/germany

IEEE Smart Grid. (2025). ***The Role of Modern Substation Automation Systems in Smart Grid Evolution - IEEE Smart Grid.*** https://smartgrid.ieee.org/bulletins/august-2021/the-role-of-modern-substation-automation-systems-in-smart-grid-evolution

INCIBE. (2025). ***Differences between OT DMZ and IT DMZ | INCIBE-CERT | INCIBE.*** (24 January 2025). https://www.incibe.es/en/incibe-cert/blog/differences-between-ot-dmz-and-it-dmz

International Renewable Energy Agency (2015). ***REmap 2030: A Renewable Energy Roadmap.*** https://www.irena.org/publications/2014/Jun/REmap-2030-Full-Report

International Trade Administration. (2025). ***Israel - Energy.*** itaadmin. https://www.trade.gov/country-commercial-guides/israel-energy

IoT M2M Council. (2023). ***Israel Electric orders Landis+Gyr smart meters - IoT M2M Council.*** https://www.iotm2mcouncil.org/iot-library/news/smart-energy-news/israel-electric-orders-landisgyr-smart-meters/

Israel Electric Corp. (2018). ***Israel Electric Corporation: For Paris 2018 Session.*** Conseil International des Grands Réseaux Électriques (Cigre).

Israel Electric Corp. (2023). ***Investor Presentation: Business update as of 12/31/2022.***

Israel Electric Corporation. (2021). ***Financial Reports: For The Nine and Three Months Ended September 30, 2021.***

Israel Energy Partnership. (2025). ***About the German-Israeli Energy Partnership.*** https://energypartnership-israel.org/about-us/

Israel National Cyber Directorate. (2019a). ***Protection of ERP systems: Recommendations for implementation.***

Israel National Cyber Directorate. (2019b). ***Exposing a Continuous Attack Campaign Against Israeli Organizations: CERT-IL.*** Reference: C-R-180. https://www.gov.il/BlobFolder/reports/continuous-attack/en/C-R-180%20(002)

Israel National Cyber Directorate. (2021). ***Managing the Risk: Full Applied Guide to Organizational Cyber Defense: Cyber Defense Doctrine 2.0.***

Israel National Cyber Directorate. (2023). ***Annual summary 2023: In the Midst of the "Iron Swords" War.*** https://www.gov.il/BlobFolder/news/booklet_yearly_summary_2023/en/booklet_yearly_summary_2023_eng

Israel National Cyber Directorate. (2024a). ***"Iron Swords" War in Cyber Sphere: Insights, Recommendations and Mitigations.*** V1.0. https://www.gov.il/BlobFolder/reports/publish_2412/en/report2412en

Israel National Cyber Directorate. (2024b). ***Cyber information no. 36 ICS-OT.***

Israel National Cyber Directorate. (2024c). ***Cyber supply chain - description of the methodology of the National Cyber Directorate: Department of Policy and Strategy.***

Julian, H. L. (2021). IEC Transfers Systems Operation Unit to 'Noga'. ***The Jewish Press – JewishPress.Com.*** https://www.jewishpress.com/news/business-economy/iec-transfers-systems-operation-unit-to-noga/2021/11/01/

Kapersky. (2025a). ***What is the Cryptolocker Virus?.*** https://www.kaspersky.com/resource-center/definitions/cryptolocker

Kapersky. (2025b). ***Stuxnet Definition & Explanation.*** https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet

kgi-admin. (2023). ***Top five transmission substation projects in Israel.*** https://www.power-technology.com/data-insights/top-five-transmission-substation-projects-in-israel/

Knupper, F. (2017). ***Cyber-Oase in der Wüste.*** https://www.juedische-allgemeine.de/israel/cyber-oase-in-der-wueste/

Knüsel, L., & Richard, P. (2022). ***Die Datenökonomie in der Energiewirtschaft: Eine Analyse der Ausgangslage und Wege in die Zukunft der Energiewirtschaft durch die Datenökonomie.***

KPMG. (2025). ***Challenges for Grid Operators in Germany.*** https://hub.kpmg.de/de/herausforderungen-fuer-netzbetreiber-in-deutschland

Kreutzmann, H., & Vollmer, S. (2014). ***Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP): Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff und Energiemengen.*** SMGW.

Kumar, R., & De, M. (2024). Power system resilience quantification and enhancement strategy for real-time operation. ***Electrical Engineering***, *106*(5), 6227–6250. https://doi.org/10.1007/s00202-024-02350-7

Legal500. (2024). ***Positive developments and trends in the Israeli Energy Market – The Legal 500.*** https://www.legal500.com/doing-business-in/positive-developments-and-trends-in-the-israeli-energy-market/

Lella, I., Theocharidou, M., Tsekmezoglou, E., & Apostolos, M. (2021). ***ENISA THREAT LANDSCAPE 2021: April 2020 to mid-July 2021.***

Lockheed Martin. (2025). ***Cyber Kill Chain®***. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Mesicek, T. (2023). ***Israel Electric Corporation (IEC) and Landis+Gyr sign agreement for smart metering solutions - Landis+Gyr.*** https://www.landisgyr.eu/news/israel-electric-corporation-iec-and-landisgyr-sign-agreement-for-smart-metering-solutions/

Ministry for Social Equality (2017). ***The National Digital Program of the Government of Israel: The Digital Israel National Initiative.***

Ministry of Defense. (2024). ***National Emergency Management Authority (NEMA).*** https://english.mod.gov.il/Departments/Pages/NationalEmergencyManagementAuthority.aspx

Mitchell, G. (2021). ***Supercharged: The EuroAsia Interconnector and Israel's Pursuit of Energy Interdependence.*** https://mitvim.org.il/en/publication/supercharged-the-euroasia-interconnector-and-israels-pursuit-of-energy-interdependence/

MITRE ATT&CK. (2024a). ***WannaCry, Software S0366 | MITRE ATT&CK®.*** (31 December 2024). https://attack.mitre.org/software/S0366/

MITRE ATT&CK. (2024b). ***Agent Tesla, Software S0331 | MITRE ATT&CK®.*** https://attack.mitre.org/software/S0331/

MITRE ATT&CK. (2024c). ***INCONTROLLER****, Software S1045* (2024). https://attack.mitre.org/software/S1045/

MITRE ATT&CK. (2024d). ***APT33, HOLMIUM, Elfin, Peach Sandstorm, Group G0064 | MITRE ATT&CK®.*** https://attack.mitre.org/groups/G0064/

MITRE ATT&CK. (2024e). ***Matrix - ICS | MITRE ATT&CK®***. https://attack.mitre.org/matrices/ics/

Mizrahi, O., Gal, N., Cohen, G., & Shani, G. (2024). ***We Need a New Concept for the Security of Electrical Systems in Israel in Emergencies and Routine Times.*** Special Publication.

NABEG. (2025). ***NABEG - Netzausbaubeschleunigungsgesetz Übertragungsnetz.*** https://www.gesetze-im-internet.de/nabeg/BJNR169010011.html

Nationales Cyber-Abwehrzentrum. (2024). https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html

Nature (2023) ***Clean energy can fuel the future - and make the world healthier.*** 620(7973), 245. https://doi.org/10.1038/d41586-023-02510-y

Nevo. (2024). ***Law for the Regulation of Security in Public Bodies, 1998: Current version as of: 08-07-2024.*** https://www.nevo.co.il/law_html/law00/71736.htm

Next Kraftwerke. (2025). ***What is a balancing group? Find out everything about balancing authorities ✓stabilizing the grid ✓ forecasts ✓and the role of renewables ✓Learn more now.*** https://www.next-kraftwerke.com/knowledge/balancing-group

Nhede, N. (2017). *Data communications:* ***Israel modernises data communications network.*** https://www.smart-energy.com/regional-news/africa-middle-east/data-communications-israel-ciena/

Nhede, N. (2019). Smart meters enabling a new era for power and utilities industry. ***Smart Energy International.*** https://www.smart-energy.com/industry-sectors/smart-meters/smart-meters-enabling-a-new-era-for-power-and-utilities-industry/

OECD. (2025). *Full Report.* https://www.oecd.org/en/publications/accelerating-climate-action-in-israel_fb32aabd-en/full-report.html

OpenKRITIS (2024). ***OpenKRITIS - Informationsplattform für KRITIS und NIS2.*** (26 August 2024). https://www.openkritis.de/

Paganini, P. (2022). ***A cyber-attack forced the wind turbine manufacturer Nordex Group to shut down some of IT systems.*** https://securityaffairs.com/129875/security/a-cyber-attack-forced-the-wind-turbine-manufacturer-nordex-group-to-shut-down-some-of-it-systems.html

Pansini, A. J. (2005). Chapter 1. The Transmission and Distribution System. In ***Guide to Electrical Power Distribution Systems*** (pp. 1–12).

Petersen, T., Stock, J., & Federrath, H. (28 July 2023). ***Bedrohungsszenarien für Energieinfrastrukturen.*** Arbeitspapier im Rahmen des Norddeutschen Reallabors. Universität Hamburg.

Pfendler, A., Freiberger, A., Gemsjäger, B., Biele, C., Schneider, C., Zipperling, E., Nowack, F., Pfeifer, F., Leugner, J., Kleimaier, M., Speh, R., Rasti, S., Wingender, S., Benz, T., & Beerens, W. (November 2022). ***Zukunftsbild Energie.*** VDE Studie.

POLITICO. (2024). ***Why energy is Israel's weak spot.*** https://www.politico.eu/article/israel-tel-aviv-energy-middle-east-power-grid-attacks-civilian/

Poudineh, R., Brandstätt, C., & Billimoria, F. (2022). Evolving Roles in Distribution Networks: Resource Coordination and Control Under the Emergence of the Distribution System Operator. In R. Poudineh (Ed.), ***Electricity Distribution Networks in the Decentralisation Era: Rethinking Economics and Regulation*** (pp. 25–43). Springer International Publishing AG. https://doi.org/10.1007/978-3-030-98069-6_3

Power Plus Communications AG. (2020). ***LTE Smart Meter Gateway - Power Plus Communications AGPower Plus Communicationa AG.*** https://www.ppc-ag.de/en/produkte/smart-meter-gateways/lte-smart-meter-gateway/

POWERGRID International. (2025). ***Israel Electric Corporation to use dynamic grid monitoring.*** https://www.power-grid.com/td/israel-electric-corporation-to-use-dynamic-grid-monitoring/

Proaktor, G., Kamara, R., & Sterzer, T. (2023). ***Israel's Second Biennial Update Report.***

Proofpoint. (2022). ***Cyber Espionage in the South China Sea | Proofpoint US.*** https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea

Reuters. (2024). ***Years-long wait for permits blocking European wind farms, industry says.*** https://www.reuters.com/sustainability/years-long-wait-permits-blocking-european-wind-farms-industry-says-2024-07-04/

Sakai, R. T., Almeida, C. F. M., Rosa, L. H. L., Kagan, N., Pereira, D. d. S., Medeiros, T. S., Kagan, H., Cruz, M. R. d., Júnior, J. A. A., Gemignani, M. M. F., Silva, G. T. A. d., & Brito, J. A. S. (2022). Architecture Deployment for Application of Advanced Distribution Automation Functionalities in Smart Grids. ***Journal of Control, Automation and Electrical Systems***, *33*(1), 219–228. https://doi.org/10.1007/s40313-021-00799-6

Schuster, S., Düser, M., Herr, C., Ostertag, M., Steinke, F., & Tusch, J. (2024). ***Mehr Resilienz für die Strom- und Kommunikationsnetze.*** VDE Impulspapier.

Schwarz, L. (2023). ***Themenroadmap der Branchenplattform Cybersicherheit in der Stromwirtschaft.***

Science|Business. (2025). ***Israel Innovation Authority and PLANETech present climate-tech innovation report.*** https://sciencebusiness.net/network-updates/israel-innovation-authority-and-planetech-present-climate-tech-innovation-report

ScienceDaily. (2025). ***Diversity can prevent failures in large power grids | ScienceDaily.*** https://www.sciencedaily.com/releases/2021/04/210401211639.htm

Shakhak, M. (2023). ***Renewable energy in Israel 2023.***

Shaping Europe's digital future. (2025a). ***Cyber Resilience Act.*** https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Shaping Europe's digital future. (2025b). ***Digitalisation of energy: best practices for data sharing.*** https://digital-strategy.ec.europa.eu/en/news/digitalisation-energy-best-practices-data-sharing

Shaping Europe's digital future. (2025c). ***NIS2 Directive: new rules on cybersecurity of network and information systems.*** https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Sonnen. (2025). ***sonnen to build the largest virtual power plant | sonnen.*** https://sonnengroup.com/press/europes-largest-vpp/

SPAMfighter. (2025). ***Virus Attack on Integral Energy Threatens Power Grid.*** https://www.spamfighter.com/News-13305-Virus-Attack-on-Integral-Energy-Threatens-Power-Grid.htm

Spence, M. (2024). Power demand from AI, EVs and Big Tech is now the energy sector's No. 1 concern. ***MarketWatch.*** https://www.marketwatch.com/story/power-demand-from-ai-evs-and-big-tech-is-now-the-energy-sectors-no-1-concern-6be1bcc1

Stancu, A.-I., & Pavel, T. (2023). Unveiling Israel's Cyber Legal Landscape A Comprehensive Analysis of Cybersecurity Regulations and Policies. In ***Perspectives of Law and Public Administration*** (Issue 4, Volume 12, pp. 644–650).

STATE OF ISRAEL PRIME MINISTER'S OFFICE. (2017). ***Israel National Cyber Security Strategy in Brief.***

Statista. (2025a). ***Germany: renewable capacity targets by source 2030 | Statista.*** https://www.statista.com/statistics/1468460/renewable-capacity-targets-by-source-germany/

Statista. (2025b). ***Redispatchmaßnahmen im deutschen Übertragungsnetz 2023 | Statista.*** https://de.statista.com/statistik/daten/studie/916903/umfrage/volumen-redispatchmassnahmen-im-deutschen-uebertragungsnetz/

Statista. (2025c). ***Renewable energy: power curtailment Germany 2023 | Statista.*** https://www.statista.com/statistics/1332954/renewable-energy-power-curtailment-germany/

Statista. (2025d). ***Topic: Renewable energy in Germany.*** https://www.statista.com/topics/5069/renewable-energy-in-germany/

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). ***Guide to Operational Technology (OT) security.*** https://csrc.nist.gov/News/2023/nist-publishes-sp-800-82-revision-3 https://doi.org/10.6028/NIST.SP.800-82r3

Stoupis, J., Rodrigues, R., Razeghi-Jahromi, M., Melese, A., & Xavier, J. I. (2023). Hierarchical Distribution Grid Intelligence: Using Edge Compute, Communications, and IoT Technologies. ***IEEE Power and Energy Magazine***, *21*(5), 38–47. https://doi.org/10.1109/MPE.2023.3288596

Strongin, R. (2014). ***Be'er-Sheva: A New, International Leader in CyberTech.*** https://americansforbgu.org/beer-sheva-new-international-leader-cybertech/

Surkes, S. (2020a). ***With $22 billion plan, Israel ups 2030 renewable energy target from 17% to 30%.*** Times of Israel. https://www.timesofisrael.com/israel-ups-2030-renewable-energy-target-from-17-to-30-at-cost-of-22-billion/

Surkes, S. (2020b). ***Cabinet greenlights target of 30% renewable energy by 2030.*** https://www.timesofisrael.com/cabinet-greenlights-target-of-30-renewable-energy-by-2030/

T&D World. (2024). ***Israel Electric Corporation to use Prisma Photonics system to monitor power grid.*** Abgerufen am 17. März 2025, von https://www.tdworld.com/test-and-measurement/article/21258214/israel-electric-corporation-to-use-prisma-photonics-system-to-monitor-power-grid

Tabansky, L. (2020). Israel Defense Forces and National Cyber Defense. ***Connections: The Quarterly Journal***, *19*(1), 45–62. https://doi.org/10.11610/Connections.19.1.05

Tabansky, L. (2021). Cybersecurity in Israel. In P. Cornish (Ed.), ***The Oxford Handbook of Cyber Security*** (pp. 631–648). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198800682.013.57

Takaharu, S. (2022). ***The Cyber Defense Organizations Protecting Israel's Critical Infrastructure and Related Challenges.*** Briefing Memo. Military Strategy Division, Policy Studies Department.

Tata Consultancy Services. (2025). ***IT Convergence: Exploiting the Best of Both Worlds.*** (2025). https://www.tcs.com/what-we-do/industries/energy-resources-utilities/white-paper/oi-it-convergence-unlock-value

Technology, E. (2013). Electric Power System – Generation, Transmission & Distribution of Electricity. ***ELECTRICAL TECHNOLOGY.*** https://www.electricaltechnology.org/2013/05/typical-ac-power-supply-system-scheme.html

Technology, L. (2023). ***Overview of the Israeli electricity market 2023.*** https://www.lnrg.technology/2023/08/27/overview-of-the-israeli-electricity-market-2023/

TeleTrusT - Bundesverband IT-Sicherheit e.V. (2024). ***Meldungen.*** https://www.teletrust.de/startseite/

Tesco Controls. (2025). ***Tesco Controls, Inc. on X: 'Cybersecurity priorities for IT and OT are direct opposites. So how can businesses gain the benefits of automation & IT/OT security? Read the article by Jonathon Shores and Benjamin Salt.*** https://t.co/xCXCSigGfg https://t.c/jdqSp1k2Wr' / *X*. https://x.com/tescocontrols/status/1455550468197953538

Trend Micro. (2025). ***Malware Discovered in German Nuclear Power Plant | Trend Micro (US).*** https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/malware-discovered-in-german-nuclear-power-plant

Tsagas, I. (2024). ***Israel's new PV installations hit 1.1 GW in 2023.*** https://www.pv-magazine.com/2024/03/13/israels-new-pv-installations-hit-1-1-gw-in-2023/

Umweltbundesamt. (2025). ***Renewable energies in figures.*** https://www.umweltbundesamt.de/en/topics/climate-energy/renewable-energies/renewable-energies-in-figures

UNITY Consulting & Innovation. (2025). ***Innogy.*** https://www.unity-consulting.com/de/projektstory/innogy-cyber-range-e/

VDE. (2025). ***Power Generating Plants in the Low Voltage Network (VDE-AR-N 4105).*** https://www.vde.com/en/fnn/topics/technical-connection-rules/power-generating-plants

Vega Penagos, C., Diaz, J., Rodriguez-Martinez, O., Andrade, F., & Luna, A. (2024). Metrics and Strategies Used in Power Grid Resilience. ***Energies***, *17*(1), 168. https://doi.org/10.3390/en17010168

Wagner, J., & Chadenas, O. (2022). ***Netzbetreiberumfrage Cybersicherheit: Zum Stand der Cybersicherheit im deutschen Stromnetz.*** ANALYSE.

Website of the Federal Government | Bundesregierung. (2025). ***Development of renewable energies | Federal Government.*** https://www.bundesregierung.de/breg-en/issues/sustainability/amendment-of-the-renewables-act-2060448

Weinstock, D., & Elran, M. (2017). ***Securing the Electrical System in Israel: Proposing a Grand Strategy.*** Memorandum 165. Institute for National Security Studies (INSS).

Weizenblut, J. (2024). ***The Blogs: Renewable Energy Industry Trends for 2024 and Israel Leading the Charge.*** https://blogs.timesofisrael.com/renewable-energy-industry-trends-for-2024-and-israel-leading-the-charge/

William Knowles, Daniel Prince, David Hutchison, Jules Ferdinand Pagna Disso, & Kevin Jones (2015). A survey of cyber security management in industrial control systems. ***International Journal of Critical Infrastructure Protection***, 9, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

Wrobel, S.B. (2023). ***Israel Electric sells Eshkol power plant to private group for over NIS 12 billion.*** Times of Israel. https://www.timesofisrael.com/israel-electric-sells-eshkol-power-plant-to-private-group-for-over-nis-12-billion/

Yazdandoust, M., & Golkar, M. A. (2020). Participation of Aggregated Electric Vehicles in Demand Response Programs. In A. Ahmadian (Ed.), ***Electric Vehicles in Energy Systems: Modelling, Integration, Analysis, and Optimization*** (pp. 327–357). Springer International Publishing AG. https://doi.org/10.1007/978-3-030-34448-1_14

Yehuda. (2023). ***ISRAEL ELECTRIC CORPORATION™ (IEC) AND ELECTRICAL GRID MONITORING™ (EGM) EXPAND COOPERATION TO OFFER PILOT DISTRIBUTION AND TRANSMISSION SOLUTIONS TO UTILITIES - EGM - Electrical Grid Monitoring Inc.*** https://egm.net/israel-electric-corporation-iec-and-electrical-grid-monitoring-egm-expand-cooperation-to-offer-pilot-distribution-and-transmission-solutions-to-utilities/

energypartnership-israel.org