Energy Resilience in an Era of Cyber & Physical Threats

Energy Tech Week 2026 - Partner: Yannay Institute for Energy Security - Lead: Avri Schechter
Contributors: Hila Gutfeld, Sheli Zargary, Tomer Goldenberg

Roundtable Summary

The roundtable examined how modern energy systems are becoming simultaneously more digital, more distributed, more interconnected, and more exposed. Participants emphasized that cyber, physical, operational, and geopolitical risks can no longer be treated as separate categories. The discussion moved beyond the question of preventing attacks and focused on resilience: how to design systems that can absorb shocks, continue essential service under stress, adapt in real time, and recover quickly. Recent events in Israel and abroad, including attacks on offshore energy assets, the war in Ukraine, and large-scale blackouts, were used as examples of how both hostile action and non-hostile failures can expose structural vulnerabilities in modern energy systems.

A central theme was that distributed energy resources create a dual effect. More EV chargers, smart meters, inverters, batteries, and local generation increase the attack surface and introduce vulnerabilities through common protocols and grid-edge devices. At the same time, distributed assets can strengthen resilience by enabling local generation, local balancing, and continuity when central infrastructure or transmission lines fail. Participants also emphasized that vulnerabilities and mitigation strategies differ across the electricity value chain: generation, transmission, distribution, storage, EV charging, and end-consumer assets each present different attack vectors, operational consequences, and recovery needs.

Participants also stressed that Israel has a unique base of relevant capabilities, however, the Israeli ecosystem has not dived into dedicated energy-security solutions. The main gaps identified were domain-specific energy cyber expertise, access to real energy data, testbeds and sandboxes, clearer regulation and liability, greater awareness among operators, boards and the public, and stronger commercial pathways for startups.

Core Insights from the Discussion

1. Energy resilience must be treated as a system-level challenge

Participants repeatedly argued that modern energy systems are not isolated technical assets, but interconnected ecosystems. This means that a disruption in one layer can spread to other layers. The key challenge is not only asset protection, but understanding how failures propagate across the system and how to limit cascading effects.

2. Adapted cyber solutions for offshore infrastructure

The offshore domain has been presented as a major national-security arena for Israel because the large share of the energy supply is in the sea. The discussion highlighted two complementary dimensions: the need for underwater and maritime threats solutions, and the need for clear operational decision-making when offshore energy assets face physical risk. Underwater pipelines, gas rigs, offshore renewables, and maritime infrastructure face threats from divers, unmanned underwater vehicles, autonomous vessels, and physical sabotage. The next step discussed was integrating detection with interception capabilities through defense-tech partnerships.

Energy cybersecurity requires domain-specific knowledge and solutions which are currently lacking. It needs to understand that energy works as a system that can be damaged physically and through specific cyber attacks and is vital to the continuity of the country's economy. Contrary to other domains, there is no accountability for infrastructure owners or operators to defend against threats.

3. Protocol standardization improves operations but introduces shared vulnerabilities

Common protocols used across distributed energy systems improve interoperability while also creating shared vulnerabilities. These protocols let operators connect multiple vendors and manage diverse assets, but they can also contain embedded vulnerabilities. A shared protocol weakness could affect how EV chargers communicate with operators, how batteries receive charging instructions, or how local controllers coordinate solar, storage, and load. In a distributed environment, a vulnerability in one device class can scale across many sites and become a systemic risk.

4. Distributed architecture is both a risk and a resilience asset

Decentralization presents strengths against cyber attacks and weaknesses. More devices and local assets mean more entry points for attackers and greater operational complexity.. As distributed energy resources proliferate, traditional network-focused cybersecurity monitoring may no longer be sufficient; abnormalities in power flows, charging and discharging behavior, and device operation can indicate cyber events that conventional tools may miss. Yet local generation and storage can help communities, campuses, and critical facilities continue operating when central grid infrastructure is disrupted. The October 7 context was discussed as an example in which local solar assets in southern communities remained available even when power lines were damaged. The threat profile and appropriate mitigation differ across the value chain: a single EV charger may cause limited damage, while a utility-scale battery, major generation asset, or central load can create broader grid-level consequences.

5. Resilience is broader than cybersecurity alone

On one hand, resilience should not only be understood through hostile attacks. Some of the most common and consequential disruptions come from engineering failures, unexpected demand, extreme weather, natural disasters, and large-scale infrastructure stress. The discussion also challenged the assumption that the future grid is only decentralizing: highly centralized loads and assets, including data centers and large generation facilities, may create high-consequence points of failure. Resilience therefore needs to address cyberattacks, war-related threats, natural disasters, operational failure, and demand shocks within a single framework.

6. Prevention, monitoring, and recovery must be designed together

The group did not frame prevention and recovery as alternatives, to the contrary, it suggested models with three layers: continuous monitoring to understand vulnerabilities and identify abnormal behavior; preventive measures that reduce the likelihood and speed of exploitation; and clear backup, restoration, and recovery procedures for when prevention fails. As AI accelerates both vulnerability discovery and exploitation, these layers need to become faster and more adaptive.

7. Responsibility and liability remain underdeveloped

The lack of responsibility and accountability for cyber-attacks was discussed. Many operators are expected to do what is needed, but actors are often unwilling to pay for stronger protection until the risk becomes visible. Stakeholders may not fully understand the depth of cyber-physical vulnerabilities, especially below the visible network layer. This weakens incentives to invest, complicates liability, and delays clear standards, while acknowledging awareness may itself create legal and commercial exposure.

8. Israel has strong capabilities, but lacks an energy-specific cyber space

Although Israel is a global cybersecurity and defense-tech leader, there are still too few companies and experts focused specifically on energy cybersecurity. Energy storage, EV charging, distributed energy resources, and data-center power supply require domain-specific knowledge. The expertise exists in separate places, but the connections between energy operators, cyber companies, defense capabilities, regulators, and startups are not yet strong enough.

Better solutions require access to real energy data, realistic test environments, and dedicated sandboxes. Access to operational energy data emerged as a core bottleneck. Energy-security solutions

cannot be developed and validated only in software environments; they require controlled exposure to real or realistic power flows, device behavior, protocol data, operational logs, and anomalies, which are sensitive, proprietary, and often inaccessible. Without controlled access to datasets and testbeds, startups cannot validate products, researchers cannot discover vulnerabilities responsibly, and operators may remain unaware of hidden risks.

Potential Action Items and Recommendations

- **Create an energy-security sandbox**
  Develop a controlled testbed for EV charging, battery storage, solar inverters, energy management systems, industrial control systems, and grid-edge devices. The sandbox should allow startups, researchers, utilities, and regulators to test cyber-physical scenarios without exposing live infrastructure.

- **Build shared but protected energy datasets**
  Establish mechanisms for anonymized or controlled access to power data, device logs, protocol data, and operational anomalies. This would help companies train and validate detection engines while respecting security and commercial sensitivity.

- **Map the full energy attack surface**
  Move from asset-by-asset protection to system-wide mapping of physical assets, digital dependencies, protocols, vendors, remote-access points, and cross-sector interdependencies. This mapping should distinguish between generation, transmission, distribution, storage, EV charging, and end-consumer assets, because each segment faces different threats and requires different mitigation and recovery strategies.

- **Develop domain-specific cyber expertise**
  Encourage training and collaboration between cybersecurity experts and energy practitioners, especially in storage, EV charging, offshore infrastructure, industrial control systems, and data-center energy supply.

- **Clarify responsibility and liability**
  Advance discussion among operators, boards, insurers, regulators, and government agencies on who bears responsibility when cyber-physical disruption affects public services and critical infrastructure.

- **Connect defense-tech capabilities to energy-security needs**
  Leverage Israeli defense and cyber capabilities for practical energy-security solutions, including offshore detection, critical infrastructure protection, early warning, digital twins, and operational resilience tools.

- **Improve market awareness and commercial incentives**
  Help operators, boards, customers, regulators, and the broader public understand the economic cost of downtime, liability exposure, and systemic risk. Greater awareness is needed so that investment in energy security becomes a business priority rather than only a regulatory or wartime necessity.

> *As the digital and physical layers of energy infrastructure converge, resilience is no longer about defending a single asset, but about building systems that can absorb shocks, adapt under pressure, and recover fast. Israel's depth in cybersecurity, defense, and energy innovation places it in a rare position to turn that challenge into the solutions the next decade will demand.*

Ignite The Spark Team
Yannay Institute for Energy Security