# What the Israel-Hamas War Means for the US Energy Supply Chain

Published 11/20/23 07:30 AM ET
Gen. James L. Jones and Brian Harrell
TheMessenger.

Director of National Intelligence Avril Haines speaks about digital threats, at the Carnegie Endowment for International Peace in April 2023 in Washington. Drew Angerer/Getty Images

Hamas's recent attack on Israel has escalated tension in the region to levels most of us haven't seen in our lifetimes. This conflict already has resulted in thousands of Israeli and Palestinian casualties, but unlike wars of the past, today these battles are being fought in new ways.

Concurrent with and in the days following the initial attacks on Oct. 7, both state-sponsored actors and sympathetic hacktivists targeted critical Israeli infrastructure to further disrupt and inhibit their ability to respond to the attacks. Less than an hour after the first rocket was fired, pro-Hamas hacktivists began attacking emergency alert systems and Israel's largest English-language newspaper.

Perhaps most concerningly, a notorious pro-Hamas group, Cyber Av3ngers, took aim at the Israeli energy supply, targeting a power grid organization, a power plant and the Israel Electric Corporation, the largest electrical power supplier in Israel and Gaza.

In short, modern conflict is no longer confined to the battlefield. These recent attacks make evident just how crucial a secure energy supply chain is, both in times of peace and in times of global instability. It is not a question of whether bad actors will attack energy supply chains, but whether we are willing to give them the chance. The U.S. energy sector must protect the nation's supply chains and critical infrastructure by integrating technology that mitigates both insider and outsider security threats.

Domestic energy infrastructure has long had vulnerabilities that have caused growing concern in recent years. As we move toward more sustainable energy infrastructure in response to climate change, these new and changing technologies can introduce new avenues for threats to enter. When the Biden administration recently announced a $3.5 billion investment in the energy grid, Department of Energy Secretary Jennifer M. Granholm stated, "The grid, as it currently sits, is not equipped to handle all the new demand," adding, "We need it to be bigger, we need it to be stronger, we need it to be smarter."

As the electric grid transforms and relies more on renewable energy solutions, components such as solar panels present a new potential attack surface through vulnerable inverters susceptible to planted malware. If an inverter's software is not updated and secure, its data could be stolen and manipulated by an adversary, potentially compromising key critical systems or embedding code in the inverter that could spread malware into the larger power system.

While the immediate energy concern is still centered in Israel, as the conflict continues — and especially if it escalates — the United States and other allies of Israel may be at risk as well. Already, a Palestinian hacker group encouraged infiltration in the United States in addition to Israel. When American private and public infrastructure can be targeted from anywhere, and at any moment, leaders have a responsibility to anticipate and prevent disruptions.

Strategic anticipation and prevention means being attentive to threats closer to home as well. Within our borders, individuals with access to the supply chain could compromise, damage, or disrupt the flow of components, products or information and, in so doing, cripple the energy grid.

Leaders should be mindful of this reality and deliberate in their insider threat mitigation strategy. This entails developing programs that use continuous monitoring tools to identify anomalous activities and malicious behavior before they lead to harmful outcomes.

Especially in times of international precarity, we must operate with the highest level of due diligence and put proactive risk identification technologies in place to ensure that no single bad actor can take advantage of America's energy infrastructure to threaten national security. Machine-learning technologies can analyze indicative data such as policy violations and criminal activity to support this integrated insider-threat deterrence, detection and mitigation strategy.

The recent examples of cyberattacks in Israel bring to light just how sudden such disruptions can be. As this and other current and potential conflicts involving Russia and China threaten to further destabilize the geopolitical climate, the need to protect the U.S. energy grid must be considered an essential part of any national security strategy.

The war of today is all-encompassing. The front lines are not just on the battlefield, but in our data and supply chains. Technology has become an essential defense tactic to address these national security threats.

What we do now matters. If we wait until there is an active attempt to disrupt American supply chains, it will be too late. We must use the technologies already at our disposal, and move quickly to bolster domestic supply chains for more secure energy infrastructure. Making these changes now will keep us from looking back on this moment and wishing we had done more.

*Gen. James L. Jones is the founder of Jones Group International, a former national security adviser to the President of the United States, and a board member for ClearForce, a people-risk technology company based in Vienna, Virginia.*

*Brian Harrell is the former Assistant Secretary for Infrastructure Protection at the Department of Homeland Security.*