Brown & Brown

PROPERTY& CASUALTY

Impact of Military Conflicts on Cyber Risk

By Christopher Keegan and Britt Eilhardt

Recent military engagements involving Israel, Iran and the United States have prompted heightened alerts from government agencies and the cybersecurity community. Organizations are urged to remain vigilant against potential cyberattacks originating from Iran, particularly those targeting Western critical infrastructure. Both state-sponsored actors and independent hacktivist groups are considered potential threats.

Increased Cyber Risks Predicted

Congress has long recognized Iran's cyber capabilities. Following the Stuxnet incident—which targeted Iran's nuclear centrifuge systems—Iran significantly escalated its cyber operations. Notably, in 2012, Iranian actors deployed destructive malware against Saudi Aramco, disabling 30,000 computers and temporarily cutting the company's oil production in half.

A joint bulletin issued on June 30, 2025, by the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, the NSA and the Department of Defense warns that Iranian-affiliated cyber actors may soon launch cyber operations targeting U.S. networks and devices.

Over the past two years, Palo Alto Networks' Unit 42 has tracked a steady expansion of Iranian-backed cyber activity. These actors have increasingly targeted critical infrastructure, supply chains, vendors and service providers. The most common tactics include distributed denial-of-service (DDoS) attacks and destructive malware, such as data wipers capable of rendering systems inoperable and requiring replacement of hardware.

Security experts have observed a particular focus on operational technology (OT) systems, especially within the energy and utilities sectors. Some Iranian-aligned groups have been linked to attacks on water systems and the defacement of industrial control systems.

Experts are urging IT and OT security teams to maintain heightened awareness, especially during weekends and off-hours, when cyberattacks are more likely to occur. The SANS ICS Five Critical Controls provide a practical and widely respected framework for organizations seeking to strengthen their OT cybersecurity posture.

Cyber War Coverage Focus

If cyberattacks materialize, the applicability of war exclusion clauses in cyber insurance policies will likely come under scrutiny. These exclusions vary significantly between insurers in both structure and intent. Whether a claim is covered may depend on specific factors such as:

- The geographic location of the affected systems
- Attribution of the attack to Iran or affiliated groups
- The degree of connection between the cyber event and recent military actions
- Formal recognition of the use of force by states and intergovernmental organizations

Attribution remains a challenge, as state actors often operate through proxies and deny direct involvement. As the physical conflict subsides, questions may arise about whether subsequent cyber incidents are still linked to acts of war.

In response to these evolving risks, some insurers are considering extended cyber war coverage. At least one market has introduced a wraparound program to address collateral cyber damage where it might be excluded under current programs. As such, reviewing war exclusions and exploring enhanced coverage options should be a priority for organizations negotiating cyber insurance policies. The current geopolitical climate underscores the need for a fresh and thorough review.

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com