AXIS / Technology

Practical Guidance

# When Cyber Becomes Warfare:

## Lessons from the Iran-Linked Attack on Stryker

Why every Western company must reassess cyber exposure in a geopolitical context

### From Cybercrime to Strategic Disruption

The Iran-linked cyberattack on Stryker marks a shift away from traditional, financially motivated cybercrime. Unlike ransomware events, there was no clear attempt to monetize the intrusion. Systems were disrupted, data was exfiltrated, and importantly, data and infrastructure were reportedly intentionally deleted or rendered unusable. The objective was impact, not payment.

Stryker, a global medical technology company embedded in healthcare delivery and infrastructure, represents the type of organization whose disruption carries consequences beyond its own balance sheet, making it a strategically relevant target within a broader geopolitical context, rather than simply a victim of opportunistic cybercrime.

Recent reporting indicates that this activity was not isolated. The Stryker incident forms part of a broader campaign of Iran-linked attacks targeting multiple U.S. industrial and infrastructure-related organizations, suggesting coordinated activity rather than a single opportunistic breach.

Most notably, this reflects a broader evolution in cyber risk. Private companies are increasingly being drawn into geopolitical conflict, not because of their own actions, but because of where they operate or who they are associated with. In this environment, the line between cybercrime and cyber warfare is becoming increasingly blurred.

### Why This Matters: A Structural Shift in Loss

Destructive attacks fundamentally change the loss dynamic. Where ransomware allows for recovery (even if costly), these events can eliminate the recovery path entirely.

Data may be permanently lost, backups compromised, and systems require full rebuild rather than restoration.

This shift exposes a key limitation in traditional cyber insurance:

- coverage is designed to restore what exists, not replace what is gone.

### The Coverage Gap: Restoration vs. Recreation

Most policies are structured to respond to ransomware and malware events through data restoration, returning systems to their pre-loss state using backups. However, where data is intentionally destroyed, the loss shifts to the recreation of that data and its underlying business value, which is often not covered.

While data recreation coverage is available, it is not standard and is typically limited to select insurers. As these types of attacks become more prevalent, the distinction between restoration and recreation is becoming increasingly significant.

## The War Exclusion Problem: When Attribution Breaks Coverage

At the same time, these events raise a more complex structural issue: the applicability of war exclusions.

Where attacks are linked directly or indirectly to state-aligned actors, insurers may look to apply war or war-like exclusions. However, modern cyber conflict rarely fits neatly within traditional definitions of warfare. Attribution is often uncertain, and many attacks are carried out through proxy groups operating in a grey zone between state and non-state actors.

This creates a fundamental tension:

1. The most severe and systemic cyber events are increasingly those most likely to trigger coverage disputes.
2. As campaigns targeting Western infrastructure and industrial companies expand, the question is no longer whether war exclusions apply, but how they will be interpreted when the lines between state and non-state activity are intentionally blurred.

## What This Means Now

The Stryker incident, and the broader pattern of activity against U.S. industrial targets, highlights a shift that is still unfolding.

Cyber risk is no longer purely operational or financially motivated; it is increasingly geopolitical in nature.

For companies, this raises two immediate considerations:

1. Whether their coverage responds in a destructive loss scenario where data must be recreated, not restored
2. Whether their policy wording provides clarity, or ambiguity, when events are linked to state-aligned actors

## Takeaway: A Developing Risk, Not a Hypothetical One

This is not a future risk, it is a developing one.

As tactics shift toward destruction over disruption, and as attribution becomes more complex, the gap between how cyber risk manifests and how it is insured is widening.

The Stryker event is an early signal of where this is heading.

**For companies operating in a more volatile cyber environment, the question is no longer if exposure exists, but whether coverage is structured to respond when it matters most.**

**Contact us for assistance with aligning your cyber coverage to emerging geopolitical risk today.**


**Contact Us**

Chris Jones
Account Executive,
Mining & Technology
+1 (778) 788-2853
Chris.Jones@axisinsurance.ca

Clive Bird
Senior Vice President,
Mining & Technology
+1 (604) 817-8072
Clive.Bird@axisinsurance.ca

Stacey Copeland
Vice President,
Mining & Technology
+1 (604) 619-7775
Stacey.Copeland@axisinsurance.ca

Tristan Smith
Business Development Specialist,
Mining & Technology
+1 (416) 885-0671
Tristan.Smith@axisinsurance.ca