RT ProExec

Iran, Cyber War, and Your Policy:
War Exclusions, Coverage Implications, and What Policyholders Need to Know Now

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

EXECUTIVE SUMMARY

Since the U.S.-Israeli military campaign against Iran began on February 28, 2026, Iran-linked hacking groups have launched a wave of cyberattacks against commercial and government targets across multiple countries. The most significant incident to date involved a destructive wiper attack against a Fortune 500 medical device manufacturer, in which a state-aligned threat actor claimed to have wiped over 200,000 devices and forced the company to shut down operations in dozens of countries. EKG transmission systems used by emergency responders went down in at least one U.S. state. This was not ransomware. It was a destructive wipe publicly claimed by the threat actor as a form of geopolitical retaliation.

That attack was not an isolated event. Since the conflict began, Iran-linked groups have targeted data centers in the Middle East, industrial facilities in Israel, airport systems in Kuwait and the Persian Gulf, government websites across multiple countries, a nuclear research facility in Poland, and a major Israeli university. Iranian state media has published a list of major U.S. technology companies it considers legitimate targets, and pro-Iranian hackers have openly discussed targeting cloud infrastructure that supports U.S. military operations.

For cyber insurance policyholders, these events represent a turning point. The war exclusion frameworks embedded in most standalone cyber policy are no longer theoretical. They are now being tested by real-world events that sit squarely at the intersection of geopolitical conflict and commercial cyber risk. This article analyzes the key insurance implications and outlines what retail brokers and their insureds should consider evaluating in their current and upcoming cyber placements.

1. What Is Happening: The Current Cyber Threat Landscape

THE HEADLINE ATTACK

On March 11, 2026, an Iran-linked hacking group known as Handala claimed a destructive cyberattack against a large, publicly traded U.S. medical device manufacturer with over $20 billion in annual revenue, approximately 50,000 employees, and operations spanning more than 60 countries. The company's products include surgical instruments, orthopedic implants, neurotechnology systems, hospital beds, defibrillators, and ambulance equipment used in hospitals worldwide.

In the early morning hours, employees across the United States, Europe, Asia, and Australia discovered that their corporate devices had been wiped. Laptops, phones, and servers enrolled in the company's device management system were remotely reset. Company login pages were defaced with Handala's logo, and the group posted a manifesto on social media claiming responsibility. The group stated the attack was retaliation for a missile strike on an elementary school in the Iranian city of Minab on February 28, 2026, the first day of the military campaign.

Handala claimed to have wiped over 200,000 systems, servers, and mobile devices, and to have exfiltrated 50 terabytes of data before executing the wipe. The targeted company filed a Form 8-K with the SEC acknowledging the cybersecurity incident and stating it had caused global disruption to the company's Microsoft environment, including disruptions to order processing, manufacturing, and shipping.

THE ATTACK VECTOR: WEAPONIZING DEVICE MANAGEMENT

What makes this attack technically significant is the method used. According to multiple cybersecurity investigators, including reporting from KrebsOnSecurity and analysis by Sophos and Palo Alto Networks, Handala did not deploy traditional wiper malware in the initial phase. Instead, the attackers compromised high-privilege administrative credentials for the company's Microsoft Intune environment. Intune is a cloud-based mobile device management (MDM) platform that IT departments use to enforce security policies and manage corporate endpoints from a single console.

By gaining administrative access to Intune, the attackers issued legitimate remote wipe commands to every enrolled device simultaneously. This is the same functionality IT administrators use when a corporate device is lost or stolen. The wipe was executed through authorized administrative channels, which means traditional endpoint detection tools may not have flagged the activity as malicious. Employees who had enrolled personal phones under the company's Bring Your Own Device (BYOD) policy also lost personal data, photos, eSIM configurations, and two-factor authentication apps when their devices were factory reset.

A BROADER WAVE OF ATTACKS

The medical device attack was the most operationally significant incident, but it was far from the only one. Since the conflict began on February 28, 2026, Iran-aligned groups have conducted an escalating campaign of cyberattacks across multiple sectors and geographies. Palo Alto Networks' Unit 42 research team has tracked dozens of pro-Iran hacktivist groups claiming attacks since the war began, mostly targeting critical infrastructure.

Known incidents and claimed attacks include: Iranian drone strikes damaging Amazon Web Services data centers in the UAE and Bahrain, causing structural damage and disrupting power delivery to cloud infrastructure. Attacks against Israeli payment systems and industrial facilities. Shutdown of Kuwaiti government websites, including Armed Forces and Ministry of Defence portals, by the Islamic Cyber Resistance (313 Team). Cyberattacks on airport systems in Kuwait, Bahrain, Saudi Arabia, and the UAE by the pro-Iran group DieNet. A claimed breach and data wipe at the Hebrew University of Jerusalem. An attempted cyberattack on Poland's National Centre for Nuclear Research, potentially linked to Iran. The installation of backdoors on networks of several U.S. companies by Iranian hackers in late February, detected by researchers at Symantec and Carbon Black. Coordination between pro-Russian hacker group NoName057(16) and Iranian hacktivists targeting Israeli defense and municipal organizations, including defense contractor Elbit Systems.

Iran's Islamic Revolutionary Guard Corps has publicly warned that the offices and infrastructure of U.S. companies with links to Israel and whose technology has been used to assist military operations will be targets. Iranian state-linked media published a list of major U.S. technology companies named as potential targets, including several of the largest cloud, enterprise software, and defense technology providers in the world.

2. The Threat Actors: Iran's Cyber Apparatus

The primary group behind the medical device attack, Handala, first surfaced in late 2023, initially presenting itself as a pro-Palestinian hacktivist group. Cybersecurity researchers, however, widely assess it as a front persona for Void Manticore, a state-sponsored actor operating under the direction of Iran's Ministry of Intelligence and Security (MOIS). Palo Alto Networks' Unit 42 research team has published detailed analysis linking Handala to Void Manticore, and further research suggests significant operational overlap with Scarred Manticore (also known as OilRig or APT34), another MOIS-affiliated advanced persistent threat group.

Handala is not the only group in play. Iran's cyber operations in the current conflict involve multiple state-linked and proxy actors. MuddyWater, another MOIS-affiliated group, has been targeting telecommunications, oil and gas, and government organizations as an initial access broker, collecting credentials and passing them to other attack groups. Hydro Kitten, operating on behalf of the IRGC, has indicated plans to target the financial sector. Pro-Iranian hacktivist groups with ties to Iraq, North Africa, and the broader Middle East have conducted operations against government and military targets across Kuwait, Romania, Bahrain, and Israel.

Critically, pro-Russian hacker groups have also aligned with Iranian operations. NoName057(16), a well-documented Russian hacktivist group, coordinated joint attacks with Iranian hacktivists against Israeli defense organizations in the first week of the conflict. Researchers at CrowdStrike have detected a broader surge of activity from Russian hackers in support of Tehran since the war began.

Key Threat Context
Cybersecurity analysts describe the medical device wiper attack as the first confirmed significant instance of Iranian cyber retaliation against a U.S. company since the war began. Analysts at Sublime Security have characterized it as a leading indicator, noting that additional Iranian state-nexus groups have likely attempted or will attempt similar operations in the near term. Former CISA Director Chris Krebs has described the current posture as an all-hands-on-deck approach by Iran, with state military, intelligence, proxies, hacktivists, and sympathizers all actively targeting adversaries. The breadth and coordination of these operations is unlike anything the market has seen from Iran in prior conflicts.

3. War Exclusions Are No Longer Theoretical

The current wave of attacks reflects a scenario frequently cited by carriers when drafting cyber war exclusion frameworks: state-aligned threat actors retaliating during an active military conflict. Whether a given cyber policy covers these types of events depends entirely on which war exclusion framework the carrier uses. This is not a uniform standard across the market. There are meaningful structural differences between carriers, and those differences will impact claims outcomes.

MODERN FRAMEWORKS VS. LEGACY EXCLUSIONS

Carriers that have adopted modern cyber war exclusion frameworks generally define excluded conduct as hostile cyber activity directed or controlled by a sovereign state as part of a war, and then carve back coverage for insureds whose own systems are not physically located in an "impacted state." These frameworks use concepts like "Impacted State," "Hostile Cyber Activity," and geographic carve-backs that are intended to address scenarios in which a U.S.-domiciled company's systems are located outside the affected war zone. A number of leading cyber carriers have adopted this type of framework, though the specific definitions and carve-back structures vary from form to form.

By contrast, carriers using legacy exclusion language may rely on traditional kinetic war exclusions, which were designed for property and casualty policies and may not clearly address cyber events at all. Others may include only a narrow cyberterrorism carve-back without a geographic or own-system carve-back. For a policyholder whose claim arises from an Iran-linked wiper attack during an active U.S.-Iran military conflict, the absence of a geographic carve-back could create ambiguity about whether the loss is covered.

CASE STUDY: PARSING A REAL WAR EXCLUSION

To illustrate the analytical complexity, consider a war exclusion that defines "Cyber War" as a harmful act conducted using a computer system, directed against one or more computer systems, committed by or at the direction of a sovereign state, that either (1) is conducted as part of a war, or (2) causes a major detrimental impact on the functioning, security, or defense of another sovereign state through disruption of essential services.

For this particular example, presume the exclusion then carves back coverage by specifying that the exclusion does not apply to the indirect effects of such acts on a computer system operated by the insured organization (or a service provider) that is not physically located in a sovereign state suffering the major detrimental impact.

Applied to the current fact pattern: a U.S. hospital that experienced a vendor disruption from the medical device attack may argue its own systems are not in Iran (the impacted state), and that a geographic carve-back could therefore be implicated. But the analysis in this basic example turns on specific definitional questions: Does the attack qualify as being "conducted as part of a War"? Does a retaliatory cyberattack by a state-linked hacktivist group meet the "at the direction or control of a sovereign state" standard? These are questions that may be litigated.

4. Attribution: Who Decides?

Attribution has historically been the single most contentious element in any cyber war exclusion dispute. In the medical device attack, the threat actor publicly claimed responsibility and multiple cybersecurity research firms have linked the group to Iran's MOIS. But the targeted company itself has not publicly attributed the attack to a specific state actor. CISA has launched an investigation but has not issued a formal attribution statement.

Different carriers handle attribution differently. Some carriers include detailed attribution frameworks in their policy language that reference determinations by G7 intelligence agencies, FBI, DHS, or equivalent bodies. Under these frameworks, a claim may hinge on whether a recognized government authority has formally attributed the attack to a state actor. Other carriers are silent on the attribution mechanism, leaving it to the claims process or, ultimately, to litigation.

For retail brokers advising clients, the attribution question can be critical. A policyholder in healthcare or defense-adjacent industries who experiences a cyber event during this conflict period should understand whether their carrier's war exclusion requires formal government attribution, relies on the insurer's own assessment, or is ambiguous. Ambiguity may not favor the policyholder in a large-loss scenario.

5. Dependent Business Interruption Exposure

One of the possible downstream implications of the medical device attack is the Dependent Business Interruption (Dependent BI) exposure for the targeted company's customers. Every hospital, surgical center, and healthcare system that relies on that company's equipment—surgical instruments, implants, monitoring devices, ambulance technology—could have experienced a vendor disruption. The same principle applies to any organization that depends on a vendor hit by one of the current wave of attacks, whether the vendor is a medical device manufacturer, a cloud infrastructure provider, a payment processor, or any other critical supplier.

Most modern cyber policies include some form of Dependent BI or Contingent BI coverage, but the scope varies considerably. Some policies limit Dependent BI coverage to disruptions caused by IT service providers, cloud hosting companies, or technology vendors. A medical device manufacturer or industrial equipment supplier may not fit neatly into those definitions. If a hospital's policy defines covered dependent entities narrowly—for example, only covering losses caused by a failure of the insured's "cloud computing provider" or "managed service provider"—a disruption from a non-IT vendor may fall outside the coverage grant.

The Amazon Web Services data center attacks add another dimension. If AWS facilities in the Middle East are damaged by drone strikes and U.S. companies experience service disruptions as a result, the Dependent BI analysis becomes even more complex. Is a physical drone strike on a data center a "security failure" that triggers cyber Dependent BI, or does it fall under a traditional property policy? The answer depends on how the triggering event is defined in the cyber form.

Retail brokers may wish to review Dependent BI definitions with clients in advance of renewal or placement discussions. Some key questions are: Does the policy cover vendor disruptions broadly, or is coverage limited to specific categories of technology providers? Is there a requirement that the dependent entity suffer a "security failure" or "network security event," and if so, does a remote wipe triggered through a legitimate administrative tool qualify?

6. Wiper Attacks Change the Loss Profile

The absence of ransomware in the medical device attack changes the first-party coverage analysis. In a typical ransomware event, the primary first-party triggers are Cyber Extortion (ransom payment and negotiation costs) and Business Interruption (lost income during the encryption and restoration period). In a wiper attack, there is no ransom demand and no decryption key. The data is gone.

Typically, the primary first-party coverage triggers for a destructive wiper event are:

Coverage Trigger	Application to Wiper Attack
Data Recovery / Restoration	Costs to rebuild, recreate, or restore data that has been permanently destroyed. This is distinct from decryption—wiped data requires reconstruction from backups (if available) or recreation from scratch.
Hardware Replacement / Bricking	When a device is factory reset or rendered inoperable, the cost to replace, reimage, or restore the hardware. Not all carriers include bricking or hardware replacement coverage.
Business Interruption	Lost income and extra expense during the period of restoration. In the medical device attack, the disruption to order processing, manufacturing, and shipping represents direct BI exposure. For downstream customers, the trigger is Dependent BI.
Forensic Investigation	Costs to determine the scope, method, and extent of the attack. The Intune-based attack vector adds complexity here, as investigators must determine how administrative credentials were compromised and what data was exfiltrated prior to the wipe.
Notification and Regulatory	If claims of exfiltrated data are even partially accurate, targeted companies face notification obligations under applicable federal and state laws, GDPR (for companies with European operations), and potentially SEC disclosure requirements.

Carriers without bricking or hardware replacement coverage can leave policyholders with limited coverage in situations like this. Wiper attacks are not new—Iran was responsible for the Shamoon attack against Saudi Aramco in 2012, which destroyed data on over 30,000 systems, and the destructive attack on the Las Vegas Sands casino in 2014—but the current conflict has produced the most significant wiper targeting of a U.S. company in over a decade. Retail brokers should consider discussing with their clients' whether their policies would benefit from including affirmative data restoration and hardware replacement coverage, not just extortion and BI.

7. Who Moves Up the Threat Ladder?

The medical device company was likely targeted because of its business profile: a major U.S. company with military contracts, an Israeli acquisition, and a global footprint that would maximize disruption and media visibility. Handala's stated targeting criteria encompasses any organization with business ties to Israel, and Iran's IRGC has issued broader threats against U.S. companies supporting military operations.

For policyholders and their brokers, this means the following categories of companies face elevated risk during the current conflict period:

Sector	Risk Basis
Healthcare and Medical Devices	Companies manufacturing, distributing, or servicing medical equipment, particularly those with DOD/VA contracts or Israeli business relationships.
Defense Industrial Base	Defense contractors, their subcontractors, and companies providing technology, logistics, or professional services to military operations.
Critical Infrastructure	Energy, utilities, water treatment, transportation, and financial services companies. Iran's IRGC has publicly warned that infrastructure of U.S. companies linked to Israel or supporting military operations will be targeted.
Technology and Cloud Services	Companies providing cloud infrastructure, managed services, or enterprise software. Iranian state-linked media has published a list of major U.S. technology companies it considers targets, and drone strikes have already damaged cloud data centers in the Middle East.
Companies with Israeli Ties	Any U.S. company with Israeli acquisitions, subsidiaries, joint ventures, partnerships, or significant customer relationships. The targeting basis is commercial affiliation, not operational involvement in the conflict.

8. Broker Action Checklist

The developments described above underscore the importance of careful policy review in the current environment. The checklist below highlights specific issues retail brokers may consider raising with clients in connection with upcoming cyber placements, recognizing that what coverage an insured may want or prioritize will vary based on its risk profile, operations, and risk tolerance.

1. War Exclusion Framework
Determine whether the carrier uses a modern Impacted State / Hostile Cyber Activity framework with a geographic carve-back and an own-system carve-back. If the exclusion relies solely on a traditional kinetic war exclusion or a narrow cyberterrorism carve-back, it may be worth a discussion.

2. Attribution Mechanism
Determine how the carrier's war exclusion defines state-sponsored or state-directed activity, and what evidence or determination triggers the exclusion. Carriers with detailed attribution frameworks referencing government intelligence determinations may provide more predictability than those with ambiguous or silent language.

3. Dependent BI Scope
For healthcare clients and any company with critical vendor dependencies, review whether the Dependent BI coverage grant extends to medical device manufacturers, equipment suppliers, cloud infrastructure providers, and other non-IT vendors. Determine if the triggering event definition is broad enough to include a vendor's security compromise.

4. Bricking / Hardware Replacement
Determine whether the policy affirmatively addresses bricking or hardware replacement costs, in addition to data restoration, and understand how the coverage is intended to respond where device recovery costs are incurred.

5. Data Recovery vs. Extortion
Review how first-party coverage is structured, including whether Data Recovery / Restoration is triggered independently or primarily in connection with extortion-related events.

6. Geopolitical Risk Conversation
For any insured with defense contracts, Israeli business ties, critical infrastructure operations, or healthcare/medical device exposure, consider initiating a proactive conversation about their elevated threat profile during the current conflict period and the adequacy of their cyber coverage.

9. Conclusion

The current wave of Iran-linked cyberattacks is not a hypothetical scenario for insurance professionals to study at a conference. These are live events with active claims implications that will test the cyber insurance market's war exclusion frameworks in real time. The attacks demonstrate that state-aligned threat actors are willing to cause maximum commercial disruption to U.S. and allied companies as a tool of geopolitical retaliation, and that the targeting criteria extends well beyond companies directly involved in military operations.

As we continue to position cyber policies in this environment, the war exclusion framework is back at the forefront of coverage questions. When quoting an account with any healthcare, defense, or critical infrastructure exposure, consider whether the coverage would benefit from a geographic carve-back and an own-system carve-back.

In response to scenarios like these, the cyber insurance market has developed increasingly sophisticated war exclusion frameworks, including approaches that address Impacted State definitions, geographic carve-backs, and attribution. Understanding how these features operate across different policy forms can be important for policyholders. Retail brokers who can articulate these differences are often able to add significant value.

SOURCES AND CITATIONS

The factual assertions in this article are based on the following publicly available sources, accessed between March 11 and March 18, 2026. Sources are organized by the sections they primarily support.

Section 1: The Headline Attack and Attack Vector

Collier, Kevin. "Iran Appears to Have Conducted a Significant Cyberattack Against a U.S. Company, a First Since the War Started." NBC News. March 11, 2026. https://www.nbcnews.com/world/iran/iran-appears-conducted-significant-cyberattack-us-company-first-war-st-rcna263084

Lyngaas, Sean. "Pro-Iran Hackers Claim Cyberattack on Major US Medical Device Maker." CNN. March 11, 2026. https://www.cnn.com/2026/03/11/politics/pro-iran-hackers-cyberattack-medical-device-maker

Krebs, Brian. "Iran-Backed Hackers Claim Wiper Attack on Medtech Firm." KrebsOnSecurity. March 12, 2026. https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/

Cimpanu, Catalin. "Medtech Giant Offline After Iran-Linked Wiper Malware Attack." BleepingComputer. March 11, 2026. https://www.bleepingcomputer.com/news/security/medtech-giant-stryker-offline-after-iran-linked-wiper-malware-attack/

Kovacs, Eduard. "Iran-Linked Hacker Attack Disrupted Manufacturing and Shipping." SecurityWeek. March 13, 2026. https://www.securityweek.com/iran-linked-hacker-attack-on-stryker-disrupted-manufacturing-and-shipping/

Al Jazeera Staff, Reuters, and The Associated Press. "Iran-Linked Hackers Hit Medical Giant in Retaliatory Cyberattack." Al Jazeera. March 11, 2026. https://www.aljazeera.com/news/2026/3/11/iran-linked-hackers-hit-medical-giant-stryker-in-retaliatory-cyberattack

"Iran-Linked Group Says It's Behind Cyberattack on U.S. Company." TIME. March 12, 2026. https://time.com/article/2026/03/12/iran-linked-cyberattack-us-company-stryker/

Bloomberg News. "Cyberattack Shows Tactics Linked to Pro-Iranian Hacking Group." Bloomberg. March 12, 2026. https://www.bloomberg.com/news/articles/2026-03-12/stryker-attack-mirrors-tactics-long-used-in-iran-aligned-hacks

"The Attack: Enterprise Resiliency Plans Can't Ignore UEM." Forrester Research. March 2026. https://www.forrester.com/blogs/the-stryker-attack-enterprise-resiliency-plans-cant-ignore-uem/

Zetter, Kim. "Iranian Hacktivists Strike Medical Device Maker in 'Severe' Attack that Wiped Systems." Zero Day (Substack). March 11, 2026. https://www.zetter-zeroday.com/iranian-hacktivists-strike-medical-device-maker-stryker-in-severe-attack-that-wiped-systems/

Section 1: Broader Wave of Attacks

Associated Press. "Iran-Linked Hackers Take Aim at US and Other Targets, Raising Risk of Cyberattacks During War." PBS News / AP. March 12, 2026. https://www.pbs.org/newshour/world/iran-linked-hackers-take-aim-at-u-s-and-other-targets-raising-risk-of-cyberattacks-during-war

CBS News. "Iran Says Major U.S. Tech Firms Are Targets in the Middle East, with Drone and Cyberattacks Already Underway." CBS News. March 13, 2026. https://www.cbsnews.com/news/iran-war-tehran-us-tech-companies-targets-middle-east-drones-cyberattacks/

Axios. "First Cyberattacks of War Hint at Iran's Playbook Against U.S." Axios. March 17, 2026. https://www.axios.com/2026/03/17/iran-us-israel-cyberattacks-critical-infrastructure

Euronews. "How Cyberattacks Are Being Used as Weapons in the Iran War." Euronews. March 18, 2026. https://www.euronews.com/next/2026/03/18/how-cyberattacks-are-being-used-as-weapons-in-the-iran-war

All sources were accessed between March 11–18, 2026. This article does not reproduce copyrighted material; all factual claims are paraphrased from the cited sources. Specific companies referenced in the underlying source material have been anonymized where appropriate.

Section 2: Threat Actor Attribution and Government Response
DiMolfetta, David. "CISA Launches Investigation into Cyberattack." Nextgov/FCW. March 12, 2026. https://www.nextgov.com/cybersecurity/2026/03/cisa-launches-investigation-stryker-cyberattack/412079/

Palo Alto Networks, Unit 42. Research on Handala / Void Manticore threat group activity, as cited in multiple reporting sources. March 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/

Samee Ali, Safia. "Iran-Linked Hackers Tied to Cyberattack on US Company." NewsNation. March 12, 2026. https://www.newsnationnow.com/world/iran-hackers-cyberattack-stryker/

"Suspected Iran-Linked Cyberattack Hits Medical Technology Giant Amid Middle East Tensions." Industrial Cyber. March 13, 2026. https://industrialcyber.co/medical/suspected-iran-linked-cyberattack-hits-medical-technology-giant-stryker-amid-middle-east-tensions/

Axios. "Hackers Join U.S. and Israel's Fight with Iran." Axios. March 11, 2026. https://www.axios.com/2026/03/11/iran-war-trump-israel-ai-cyberattack

Sections 7–8: Geopolitical Threat Context
"Wiper Attack: What Security Teams Need to Know Now." 7AI. March 2026. https://7ai.com/stryker-wiper-attack-what-security-teams-need-to-know-now

"Cyberattack 2026: Lessons from a Global Wiper Attack." ProArch. March 2026. https://www.proarch.com/blog/threats-vulnerabilities/stryker-wiper-attack-analysis

"Wiper Attack Takes Target Offline Across 79 Countries." SafeState. March 11, 2026. https://www.safestate.com/post/handala-wiper-attack-takes-stryker-offline-across-79-countries

"Iran-Linked Hacktivist Group Hits Target in Destructive Wiper Attack." SecureWorld. March 12, 2026. https://www.secureworld.io/industry-news/iran-linked-hacktivist-group-weaponizes-microsoft-intune-in-destructive-wiper-attack-on-stryker

Insurance Journal / Associated Press. "Iran-Linked Hackers Take Aim at US, Other Targets, Raising Risk of Cyberattacks." Insurance Journal. March 17, 2026. https://www.insurancejournal.com/news/national/2026/03/17/862140.htm

All sources were accessed between March 11–18, 2026. This article does not reproduce copyrighted material; all factual claims are paraphrased from the cited sources. Specific companies referenced in the underlying source material have been anonymized where appropriate.