everbridge

Military Conflict Trend Analysis

Digital Infrastructure and the Shifting Dynamics of the Iran Conflict

March 17, 2026

Overview

On March 1, Iranian drone strikes targeted three Amazon Web Services (AWS) facilities in the Middle East, directly hitting two sites in the United Arab Emirates (UAE) and affecting a third in Bahrain through a nearby strike. While the specific facilities were not publicly identified, these attacks disrupted AWS cloud availability zones in both countries and affected infrastructure supporting data storage, cloud computing, and regional digital connectivity. The strikes took place during a broader phase of Iranian retaliation following U.S. and Israeli attacks on Iran in late February and reflected Tehran's effort to impose costs beyond the immediate battlefield. In this context, the inclusion of Gulf-based digital infrastructure in the target set suggests that the conflict is widening beyond conventional military sites to include commercially operated systems seen as strategically relevant.

More broadly, the attacks point to a widening threat environment in which commercial digital infrastructure is increasingly exposed to conflict-related disruption, particularly where it is perceived to support strategically significant technologies or operations. As the U.S. military makes greater use of artificial intelligence for functions such as analysis, targeting support, and operational decision-making, the physical infrastructure that stores, processes, and transmits data may become more attractive as a target. This raises the risk that data centers and cloud platforms will be viewed not simply as commercial facilities, but as infrastructure with potential military relevance, increasing exposure not only for defense-linked systems, but also for businesses and the wider public that rely on those same networks and services for communications, transactions, and access to essential digital tools.

Evolving Dynamics of Military Conflict

The current U.S.-Iran-Israeli war began in late February, when U.S. and Israeli strikes on Iran, launched with the stated aim of degrading the country's nuclear and ballistic missile programs, triggered a broader conflict that has since moved beyond direct military exchanges. In addition to conventional operations, the conflict is increasingly being shaped by cyber activity, economic pressure, and disruption targeting the systems that underpin routine commercial and state functions.

Iran-linked and Iran-aligned cyber activity has reportedly risen 245 percent since February 28, with much of the observed activity concentrated in banking and financial technology. That focus suggests an effort to target sectors where even limited disruption can generate economic friction, visible service interruptions, and broader public unease. Much of the activity has involved reconnaissance, infrastructure scanning, credential harvesting, and apparent preparation for distributed denial-of-service attacks, pointing to a sustained threat environment even where immediate effects remain limited. The recent cyberattack on Stryker, which disrupted the U.S. medical device company's global networks, further suggests that this pressure is not confined to the immediate theater of operations, but can also extend to major commercial entities with broader economic or symbolic significance.

Taken together, these developments suggest the conflict is evolving toward a more integrated form of asymmetric warfare in which cyber operations, infrastructure disruption, and digitally enabled military activity are increasingly interconnected. The Pentagon's growing use of artificial intelligence to support analysis and targeting may further

elevate the strategic relevance of the data, cloud services, and networked systems that underpin those capabilities. In an increasingly digital operating environment, this expands exposure not only for military-linked systems, but also for businesses, service providers, and populations that depend on the same infrastructure for essential functions.

Implications and Risk Outlook

The convergence of physical strikes on data infrastructure, disruptive cyber activity, and the growing military use of artificial intelligence suggests that commercial digital systems are likely to face sustained exposure in future phases of the conflict. As data centers, cloud platforms, and related networks become more closely associated with operational support, they may increasingly be viewed as targets with strategic value rather than as insulated commercial assets. This raises the likelihood of further attempts to disrupt infrastructure that underpins communications, logistics, financial activity, and other digitally enabled services, particularly in regions closely tied to U.S. military operations or allied technology networks

The risk may also extend beyond data centers themselves to other physical sites associated with digital infrastructure, both within the Middle East and farther afield. Telecommunications facilities, satellite ground stations, internet exchange points, cable landing stations, and supporting power systems could become more exposed where they are seen as enabling military-relevant data flows or broader operational continuity. In the Gulf, such sites face heightened vulnerability because of their proximity to the conflict and their role in supporting regional connectivity. Beyond the region, the more plausible threat in Europe or the U.S. is cyber disruption, covert sabotage, or proxy activity against infrastructure linked to digital services, rather than overt missile or drone strikes. Comparable infrastructure outside the Middle East could nevertheless face increased risk where it supports cloud services, financial platforms, healthcare systems, or critical communications with strategic or symbolic value.

For businesses and organizations, the implications extend beyond direct damage to include cascading operational disruption through third-party providers and interconnected platforms. Firms that rely on cloud infrastructure, digital payments, healthcare systems, or regional data hosting may face heightened business continuity pressures even when they are not directly connected to the conflict. The wider public is also exposed, as disruption to these sites can affect access to banking, communications, transportation, healthcare, and other essential services. Looking ahead, the conflict points to an evolving threat landscape in which increasingly digital and AI-enabled warfare is expanding the range of actors, sectors, and populations vulnerable to disruption.

Resilience and Mitigation Considerations

Organizations operating in or connected to the Middle East may need to plan for disruption that affects both digital systems and the physical infrastructure that supports them. This includes not only cyber incidents such as credential compromise, distributed denial-of-service activity, or network intrusion, but also outages tied to damage at data centers, telecommunications facilities, satellite ground stations, cable landing stations, and supporting power systems. In this environment, resilience planning is likely to be most effective where it assumes that commercially operated digital infrastructure may face both direct attack and cascading disruption across interconnected providers and services. For businesses and infrastructure operators in the Middle East, this places greater importance on understanding third-party dependencies, especially where cloud hosting, digital payments, communications, or data processing are concentrated in a limited number of providers or geographic locations. Measures such as geographic redundancy, backup communications, segmented network architecture, offline recovery capabilities, and pre-established continuity procedures may help reduce operational vulnerability. For organizations outside the region, the focus may be less on direct physical exposure and more on spillover risk through cyber disruption, vendor concentration, and dependence on globally interconnected digital infrastructure. Businesses in Europe, North America, and other external markets may benefit from reviewing whether critical services rely on providers, routes, or facilities with regional exposure,

strengthening incident response procedures for third-party outages, validating backup connectivity and payment workflows, and ensuring that essential operations can continue during disruption affecting cloud, telecom, or managed service providers.

Given the growing overlap between military, commercial, and public-facing digital systems, organizations both inside and outside the Middle East may also need to reassess whether assets previously treated as routine business infrastructure now carry greater strategic exposure. This includes examining whether data hosting arrangements, network nodes, logistics platforms, communications systems, or externally managed digital services could be perceived as operationally significant in a conflict environment shaped by cyber operations, physical targeting, and the expanding use of artificial intelligence. In practical terms, that may require a broader view of resilience that goes beyond cybersecurity alone and considers the physical location, ownership, connectivity, and strategic relevance of key infrastructure dependencies. For some organizations, this may also mean revisiting internal assumptions about what constitutes critical infrastructure, which services are truly essential to maintain, and how quickly operations could be adapted if commercially operated systems were disrupted for geopolitical rather than purely technical reasons.

Forward Outlook

In the short term, the most likely trajectory is continued pressure on commercial digital infrastructure through cyber activity, isolated physical attacks, and efforts to exploit dependence on cloud and connectivity services. Recent developments suggest a continued willingness to target commercially operated systems with strategic, economic, or symbolic value. Additional disruption is most likely to affect sectors such as finance, healthcare, logistics, and communications, particularly where organizations rely on regionally concentrated providers or infrastructure with exposure to the Middle East. Outside the region, the near-term spillover risk is more likely to take the form of cyber disruption, proxy activity, or covert sabotage than overt physical attacks.

Over the medium term, this conflict is likely to accelerate the treatment of digital infrastructure as part of the operational battlespace rather than as a protected commercial backstop. As militaries make greater use of artificial intelligence, cloud processing, and data-driven targeting tools, the physical infrastructure that supports those capabilities may be viewed more readily as a viable target set. That shift could broaden exposure beyond data centers to include telecommunications nodes, satellite ground infrastructure, internet exchange points, cable landing stations, and supporting energy systems. It is also likely to drive more active reassessment by governments and private-sector operators of what constitutes dual-use infrastructure, with increased emphasis on redundancy, geographic diversification, and closer scrutiny of provider concentration risk.

Over the longer term, the conflict may help normalize a more integrated form of asymmetric warfare in which cyber operations, limited physical strikes, and attacks on commercially operated digital systems are used together to impose costs beyond the traditional battlefield. In that environment, businesses and infrastructure operators may face a more persistent baseline of geopolitical risk tied not only to where they operate, but also to which platforms, networks, and service providers they depend on. The broader implication is that the line between military and commercial infrastructure is likely to become more contested, particularly in sectors linked to cloud services, AI-enabled tools, healthcare, finance, and critical communications. That would leave a wider range of organizations, and the publics that rely on them, exposed to disruption during future crises even where they are geographically distant from the immediate conflict zone.

Contact: GlobalInsightsTeam@everbridge.com