Working Paper

F-Series Information:
The WP-F series explores AI governance and strategic risk through comparative and historical diagnostics, examining how inherited strategic and regulatory logics break down when transferred into AI-mediated contexts.

Recommended Citation:
Wu, Shaoyuan. (2026). *Cloud Under Fire: Hyperscale Data Centers and the Rise of Cyber-Physical Warfare* (EPINOVA Working Paper No. EPINOVA–WP–F–2026–05). Global AI Governance and Policy Research Center, EPINOVA LLC. https://doi.org/10.5281/zenodo.18923621.

Disclaimer:
This working paper presents diagnostic and exploratory analysis intended to examine inherited strategic and governance logics under AI-mediated conditions. It does not constitute policy recommendations, predictive assessments, or official positions of any institution.

GLOBAL AI GOVERNANCE RESEARCH CENTER

EPINOVA

Cloud Under Fire:
Hyperscale Data Centers and the Rise of Cyber-Physical Warfare

Author: Shaoyuan Wu

ORCID: https://orcid.org/0009-0008-0660-8232

Affiliation: Global AI Governance and Policy Research Center, EPINOVA LLC

Date: March 09, 2026

Abstract

The rapid expansion of cloud computing has concentrated critical digital services within a relatively small number of hyperscale data centers operated by major technology firms. These facilities support financial systems, artificial intelligence platforms, logistics networks, and government operations, making them essential components of contemporary economic and technological systems. As a result, cloud infrastructure may increasingly represent a potential category of strategic targets in modern conflict.

This article examines the emerging militarization of digital infrastructure through the case of reported drone strikes affecting infrastructure near Amazon Web Services (AWS) cloud facilities in the United Arab Emirates and Bahrain during the 2026 U.S.–Iran conflict. Building on the concept of Digital Strategic Nodes, the paper argues that hyperscale data centers represent highly concentrated points of systemic digital dependence and may therefore become attractive targets for adversaries seeking strategic disruption.

Drawing on international relations scholarship on cyber conflict, critical infrastructure security, and cyber-physical systems, the article maps major digital infrastructure across the Middle East. The analysis identifies an expanded inventory of 28 digital strategic nodes, including hyperscale cloud regions, Internet exchange points, submarine cable landing stations, cloud interconnection facilities, and edge-distribution nodes located within the strike range of Iranian missile systems. Depending on whether secondary interconnection and edge facilities are included, the regional network comprises roughly 20–30 strategically significant nodes.

The findings suggest that contemporary warfare is increasingly characterized by cyber-physical interaction, in which kinetic attacks on digital infrastructure may produce effects traditionally associated with cyber operations. This dynamic complicates existing theories of cyber deterrence and highlights the growing strategic importance of protecting large-scale digital infrastructure in future conflicts.

Keywords: Cyber-physical warfare; cloud infrastructure; hyperscale data centers; critical infrastructure security; digital strategic nodes; cyber conflict; Middle East conflict; infrastructure targeting

Working Paper

1. Introduction

Digital infrastructure has become a foundational component of the global economy. Cloud computing platforms host financial transactions, artificial intelligence systems, logistics coordination networks, and government databases that support daily economic and political activity (Armbrust et al., 2010; Varian, 2019). Hyperscale data centers, the large computing facilities operated by firms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud, have emerged as the core architecture of this digital ecosystem (Cusumano, Gawer, & Yoffie, 2019). By concentrating vast computational capacity and data storage within a relatively small number of facilities, hyperscale cloud infrastructure now functions as critical backbone infrastructure for both economic systems and digital governance.

The growing concentration of computational capacity within hyperscale facilities raises a fundamental question for international security: **can cloud infrastructure become a strategic target in modern warfare?**

This question gained renewed attention during the 2026 U.S.–Israel–Iran conflict. Reports indicated that drone strikes attributed to Iranian forces damaged infrastructure associated with AWS data centers in the United Arab Emirates and Bahrain, causing localized service disruptions (Reuters, 2026; Associated Press, 2026). Although the incident did not produce large-scale outages, it illustrates how digital infrastructure may increasingly intersect with military strategy. In an environment where cloud platforms host a wide range of economic and governmental functions, the disruption of hyperscale data centers could potentially generate cascading effects across digital systems and regional economies.

Existing cyber conflict literature has primarily focused on digital intrusions, malware campaigns, and network exploitation (Rid, 2013; Valeriano & Maness, 2015). While this scholarship has significantly advanced understanding of cyber operations, it has largely examined cyber effects as the result of digital intrusion into computer systems. Less attention has been devoted to scenarios in which kinetic attacks on digital infrastructure produce cyber-like disruption. This question also relates to broader debates concerning the cyber offense–defense balance and the strategic effectiveness of cyber operations (Slayton, 2017).

As modern economies become increasingly dependent on cloud computing infrastructure, the physical facilities supporting digital networks may acquire growing strategic significance. In highly centralized digital architectures, disruptions affecting a limited number of infrastructure nodes may generate cascading systemic effects across financial systems, logistics networks, and government services. Understanding how such infrastructure could become integrated into military strategy therefore represents an increasingly important question for international security research.

Hyperscale cloud infrastructure represents a new category of Digital Strategic Nodes (DSNs)—highly concentrated infrastructure points whose disruption may produce cascading effects across digital networks and economic systems.

Thus, the paper addresses the following research question:

How does the physical targeting of cloud infrastructure reshape the cyber-physical dynamics of modern warfare?

To answer it, the article combines theoretical analysis with empirical mapping of digital infrastructure across the Middle East. Using the reported AWS data center incident as a case study, the paper examines how hyperscale infrastructure may become integrated into military strategy and evaluates the implications of such developments for cyber deterrence and infrastructure security.

This paper makes three contributions. First, it introduces the concept of Digital Strategic Nodes to analyze the strategic significance of concentrated digital infrastructure. Second, it provides an empirical mapping of major digital infrastructure nodes in the Middle East, demonstrating how many of these facilities fall within the strike range of regional missile systems. Third, the article contributes to cyber conflict scholarship by highlighting the growing importance of cyber-physical interactions, in which kinetic attacks on infrastructure generate effects traditionally associated with cyber operations.

2. Literature Review

2.1 Cyber Conflict and the Limits of Cyber Warfare

The study of cyber conflict has expanded rapidly over the past two decades, reflecting the emergence of cyberspace as a new domain of strategic competition (Healey, 2011). Early scholarship focused on whether cyber warfare would fundamentally transform military conflict or instead remain limited in its strategic impact (Rid, 2013; Libicki, 2009; Clarke & Knake, 2010). This debate is closely related to broader questions regarding the cyber offense–defense balance and the strategic effectiveness of cyber operations (Slayton, 2017).

Rid (2013) argues that cyber war in its pure form is unlikely to occur because cyber operations typically lack violence, political symbolism, and coercive power associated with traditional military conflict. Similarly, Valeriano and Maness (2015), drawing on empirical datasets of cyber incidents between states, find that most cyber operations remain limited in scope and rarely escalate into armed conflict.

However, other scholars emphasize that cyber operations can still generate significant strategic effects, particularly when integrated with broader military campaigns or when directed against critical infrastructure systems (Borghard & Lonergan, 2017; Lindsay, 2013; Nye, 2017). The Stuxnet operation targeting Iranian nuclear facilities demonstrated that cyber operations can produce physical consequences by manipulating industrial control systems, illustrating the growing integration of cyber capabilities into state strategy (Langner, 2011).

Despite this expanding body of research, most cyber conflict studies assume that cyber effects originate primarily from digital intrusion into computer systems rather than from physical disruption of the infrastructure that supports digital networks. As a result, relatively little attention has been devoted to scenarios in which kinetic attacks on digital infrastructure generate cyber-like disruption, such as service outages or network instability.

2.2 Critical Infrastructure and Cyber-Physical Systems

A related strand of literature examines the protection and vulnerability of critical infrastructure systems, including energy grids, telecommunications networks, and transportation systems (Lewis, 2014). These infrastructures increasingly rely on digital control systems and networked technologies, creating hybrid environments commonly described as cyber-physical systems.

Research on cyber-physical security highlights how disruptions can propagate across both physical and digital networks. For example, cyber intrusions into industrial control systems can generate cascading failures in power grids, manufacturing systems, or transportation networks (Nye, 2017). The growing interdependence between digital and physical systems has therefore become a central concern in infrastructure security.

However, much of this literature focuses on cyber-attacks producing physical effects, such as disruptions to industrial equipment or infrastructure operations. Less attention has been paid to the reverse dynamic, in which physical attacks on infrastructure generate systemic digital disruption, particularly in environments where economic and governmental systems depend heavily on centralized digital infrastructure.

2.3 Cloud Computing and Infrastructure Centralization

The rapid expansion of cloud computing has significantly transformed the architecture of global digital infrastructure. Hyperscale data centers enable technology firms to provide computing services at enormous scale while reducing operational costs through centralized infrastructure and distributed network architecture (Cusumano et al., 2019).

While this centralization improves efficiency and scalability, it also introduces potential systemic vulnerabilities. When large portions of digital services depend on a relatively small number of hyperscale facilities, disruptions affecting these locations may produce cascading effects across multiple sectors, including finance, logistics, communications, and government services.

Despite the strategic implications of this infrastructure architecture, international relations scholarship has only recently begun to examine cloud infrastructure as a potential element of geopolitical competition. As cloud platforms increasingly underpin economic activity and digital governance, hyperscale data centers may represent a new category of strategic infrastructure whose disruption could generate significant regional or global effects.

2.4 Literature Gap

Taken together, these strands of literature highlight three important insights regarding the relationship between digital infrastructure, cyber conflict, and strategic vulnerability. First, cyber conflict research has largely focused on digital intrusion as the primary mechanism through which cyber effects are generated. Second, infrastructure security studies emphasize the growing integration between cyber systems and physical infrastructure. Third, research on cloud computing demonstrates the increasing centralization of digital services within hyperscale data centers.

However, these literatures rarely intersect. In particular, limited attention has been devoted to scenarios in which kinetic attacks on centralized digital infrastructure generate systemic cyber effects. This gap becomes increasingly important as hyperscale data centers emerge as critical nodes in global digital networks.

The growing strategic importance of this gap is reinforced by the high level of concentration within the global cloud computing market. Industry estimates indicate that a small number of providers dominate global cloud infrastructure capacity. Amazon Web Services, Microsoft Azure, and Google Cloud collectively account for a majority share of global cloud services, reflecting a highly centralized digital infrastructure architecture (Synergy Research Group, 2024; Statista, 2024). As a result, a relatively small number of hyperscale data centers host computing resources and digital services used by governments, corporations, and digital platforms across entire regions.

The concept of Digital Strategic Nodes, introduced in this paper, seeks to bridge this gap by examining how concentrated digital infrastructure may become integrated into military strategy and how physical attacks on such infrastructure could generate cyber-physical disruption.

3. Digital Strategic Nodes Theory

The increasing centralization of digital infrastructure raises important questions about how network architecture shapes strategic vulnerability. In highly networked systems, infrastructure nodes that concentrate connectivity, data flows, or computational capacity may become critical points whose disruption can generate cascading effects across entire networks. As digital economies increasingly rely on cloud platforms and global data networks, certain infrastructure locations may therefore acquire disproportionate strategic significance.

Working Paper

To analyze this phenomenon, this article introduces the concept of **Digital Strategic Nodes (DSNs)**, defined as infrastructure locations whose disruption may generate disproportionate systemic effects due to their central role within digital networks. These nodes function as key junctions through which data traffic, computational resources, or network connectivity are concentrated and coordinated.

This perspective also aligns with the concept of network power, which emphasizes how actors may exercise influence by controlling key nodes within global economic and information networks (Farrell & Newman, 2019). This perspective also resonates with broader arguments about network power and infrastructure control in global political economy (Farrell & Newman, 2022). In highly networked digital systems, infrastructure nodes that combine high levels of connectivity and concentration may therefore acquire strategic significance. Control over such nodes can create asymmetric leverage within networked systems, allowing disruption at a limited number of points to generate wider systemic effects.

Examples of digital strategic nodes include hyperscale cloud data centers, Internet exchange points (IXPs), submarine cable landing stations, cloud interconnection hubs, and edge-distribution or content-delivery network (CDN) nodes.

These infrastructures serve as essential junctions within global digital networks. Because large volumes of data traffic and computing capacity pass through relatively small numbers of facilities, disruptions affecting these nodes may propagate rapidly across interconnected systems.

The DSN framework highlights two core structural characteristics of digital infrastructure.

Concentration: Hyperscale cloud data centers concentrate massive computational capacity and data storage within a limited number of physical locations. As a result, a relatively small number of facilities may support large portions of regional or global digital services.

Connectivity: Internet exchange points and submarine cable landing stations function as central hubs for network traffic, linking national and transnational communication networks. Their central position within Internet routing architecture allows them to facilitate large volumes of data exchange between networks.

When digital infrastructure combines high concentration and high connectivity, disruptions affecting these nodes may generate cascading systemic effects across digital networks and economic systems. In such environments, localized infrastructure disruption may propagate into wider network instability, service outages, or economic disruption.

From a strategic perspective, infrastructure nodes that exhibit both high concentration and high connectivity may represent attractive targets for adversaries seeking asymmetric disruption. Rather than attacking large numbers of distributed systems, actors may attempt to disrupt critical nodes whose failure could produce broader systemic consequences.

To further conceptualize this dynamic, the vulnerability of digital infrastructure can be understood as a function of both structural characteristics and strategic exposure. While concentration and connectivity describe the architecture of digital networks, the strategic risk associated with a node also depends on its geographic exposure to military strike capabilities.

In simplified conceptual form, the risk associated with a Digital Strategic Node can be expressed as:

$$\boldsymbol{DSN\ Risk \propto Concentration \times Connectivity \times Geographic\ Exposure}$$

The conceptual relationship among these variables is illustrated in **Figure 1**.

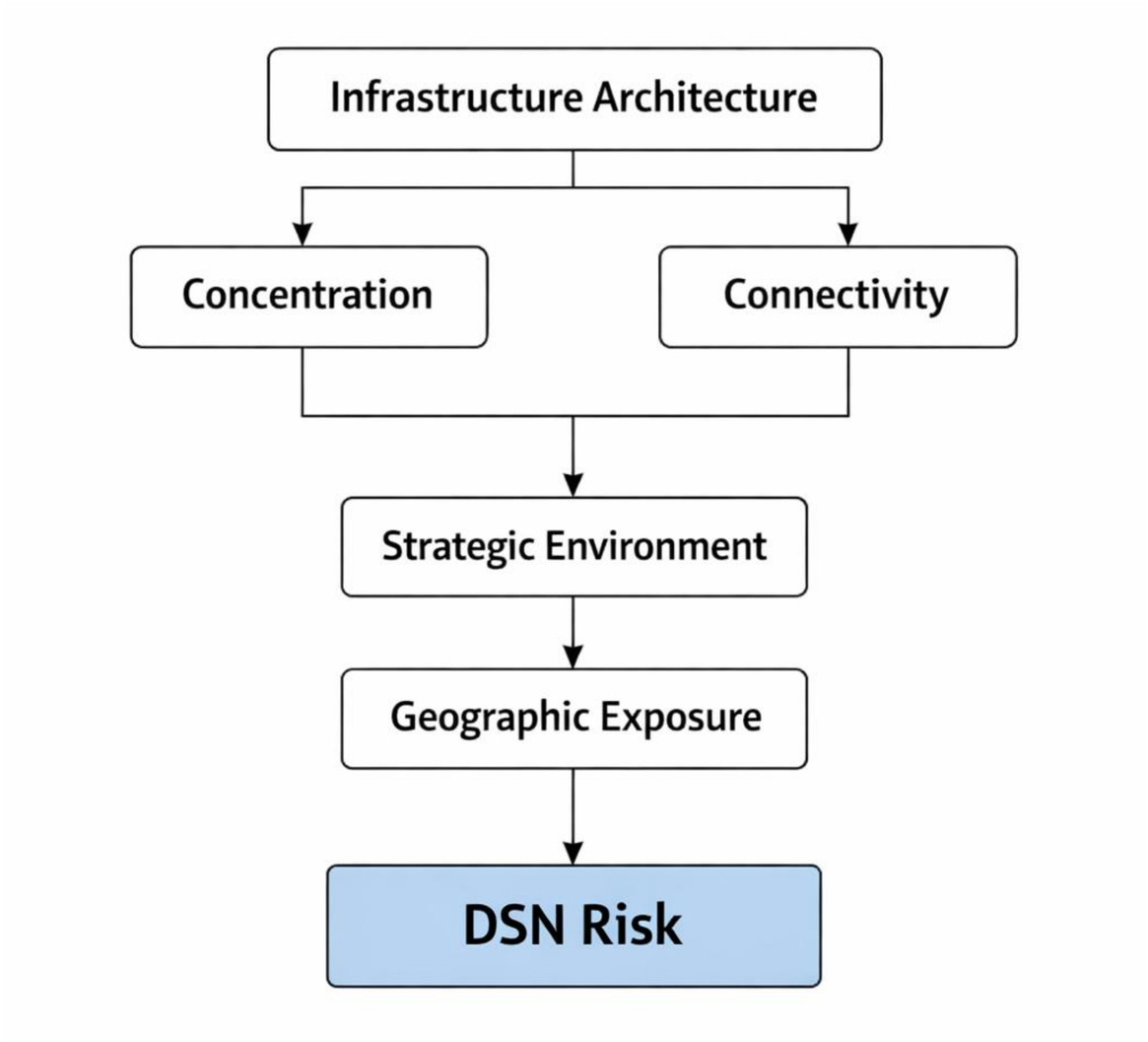

Figure 1. Conceptual model of DSN risk, illustrating how infrastructure concentration, network connectivity, and geographic exposure interact to shape strategic vulnerability.

In this framework, concentration refers to the degree to which computing capacity and digital services are centralized within a limited number of facilities. Connectivity reflects the extent to which a node functions as a junction within regional or global data networks, such as Internet exchange points or submarine cable landing stations. Geographic exposure refers to the physical accessibility of infrastructure within the strike range of conventional military capabilities, including missiles or drones.

Nodes that combine high levels of concentration and connectivity while also remaining geographically exposed to potential adversaries may therefore represent particularly attractive targets for strategic disruption. Under such conditions, localized physical attacks on a limited number of infrastructure nodes may generate disproportionate systemic effects across digital networks and economic systems.

The concept of Digital Strategic Nodes therefore provides a framework for analyzing how the architecture of digital infrastructure can shape strategic vulnerability in contemporary conflict environments.

4. Digital Infrastructure in the Middle East

Over the past decade, the Middle East has emerged as a growing hub for cloud computing infrastructure, reflecting broader transformations in the governance and globalization of digital infrastructure systems (Seabrooke & Wigan, 2021). Governments across the Gulf region have launched ambitious digital transformation strategies aimed at diversifying national economies, expanding digital services, and supporting artificial intelligence development (Varian, 2019). These initiatives have attracted major global technology firms, leading to the rapid expansion of hyperscale cloud infrastructure across several countries in the region.

Working Paper

Major hyperscale cloud regions currently operating in the Middle East include AWS Bahrain Region, AWS UAE Region, Microsoft Azure UAE, Microsoft Azure Qatar, Google Cloud Israel, and Oracle Cloud Saudi Arabia.

These facilities provide cloud services to governments, financial institutions, and technology firms across the Middle East and neighboring regions. As a result, they function as key nodes within the regional digital infrastructure architecture.

In addition to hyperscale cloud facilities, the region hosts several major Internet exchange points (IXPs) and submarine cable landing stations, which serve as critical hubs for global Internet connectivity.

Major IXPs in the region include: UAE-IX (Dubai), Saudi Internet Exchange, and Qatar Internet Exchange.

These facilities facilitate high-volume data exchange between Internet service providers and international networks, allowing regional traffic to be routed efficiently across global digital networks. Their strategic importance has also been linked to debates about the potential fragmentation of the global Internet and the geopolitical control of digital infrastructure (Mueller, 2017).

The Middle East also hosts several important submarine cable landing stations that connect regional networks to global Internet infrastructure. Key cable landing hubs include: Fujairah (United Arab Emirates), Jeddah (Saudi Arabia), Doha (Qatar), and Tel Aviv (Israel).

Together, these infrastructures form an interconnected network of digital strategic nodes that support regional and global data flows.

Mapping these infrastructures together with cloud interconnection hubs and edge-distribution facilities suggests an expanded inventory of approximately 28 digital strategic nodes across the Middle East. These include hyperscale cloud facilities, Internet exchange points, and submarine cable gateways that occupy central positions within regional digital networks.

Importantly, many of these facilities fall within the estimated 2000-kilometer strike range of Iranian medium-range missile systems. This geographic overlap creates a structural intersection between digital infrastructure and regional military dynamics. In the event of armed conflict, disruptions affecting a relatively small number of these nodes could potentially generate cascading effects across regional digital networks and cloud services.

5. Case Study: Reported Drone Strikes Near AWS Cloud Infrastructure

Reports during the early phase of the 2026 U.S.–Iran conflict indicated that drone strikes affected infrastructure located near Amazon Web Services (AWS) cloud facilities in the United Arab Emirates and Bahrain (Reuters, 2026; Associated Press, 2026; Financial Times, 2026). Some reporting also suggested that infrastructure associated with Microsoft Azure facilities in the region was discussed as a potential target during the attacks (Financial Times, 2026). The analysis relies on open-source reporting and publicly available information regarding the incident. According to these reports, the attacks damaged supporting infrastructure in the vicinity of the data centers and caused temporary service disruptions affecting regional cloud customers. Although the operational impact appeared limited and services were reportedly restored within a short period of time, the episode attracted considerable attention because of the growing strategic significance of hyperscale cloud infrastructure.

If confirmed, the episode may represent one of the earliest reported instances in which infrastructure associated with hyperscale cloud platforms operated by major technology firms was affected during an armed conflict. While telecommunications networks and broadcasting infrastructure have frequently been targeted in previous wars, large-scale cloud computing facilities have generally been regarded as civilian digital infrastructure rather than as potential objects of military action.

The strategic importance of such infrastructure is reinforced by the high level of concentration within the global cloud computing market. Amazon Web Services, Microsoft Azure, and Google Cloud collectively account for a dominant share of global cloud infrastructure capacity. As a result, a relatively small number of hyperscale data centers host computing resources and digital services used by governments, financial institutions, and private companies across entire regions.

From the perspective of the DSN framework introduced earlier, hyperscale cloud facilities exhibit two structural characteristics commonly associated with strategic infrastructure: high concentration and high connectivity. Consequently, disruptions affecting these facilities may propagate across multiple sectors simultaneously.

Several factors may help explain why cloud infrastructure could emerge as a potential target in contemporary conflict.

First, hyperscale data centers support a wide range of economic and administrative functions. Cloud platforms host financial transactions, logistics coordination systems, artificial intelligence services, and digital government infrastructure. Disruptions affecting cloud availability may therefore generate economic pressure without necessarily requiring large-scale military escalation.

Second, cloud facilities operated by major U.S. technology firms may be perceived by adversaries as components of a broader ecosystem associated with American technological influence. Because a small number of companies dominate global cloud markets, their infrastructure may be interpreted as representing elements of U.S. digital and economic power.

Third, the concentration of digital services within hyperscale facilities creates the potential for systemic ripple effects. In highly centralized digital environments, localized physical disruption affecting key infrastructure nodes may generate disproportionate operational consequences across interconnected digital systems.

Taken together, these factors suggest that hyperscale cloud infrastructure may increasingly become integrated into the strategic landscape of contemporary conflict, particularly in regions where dense digital infrastructure overlaps geographically with areas of military confrontation.

6. Cyber-Physical Warfare

The AWS incident highlights an emerging form of warfare that may be described as cyber-physical warfare. While traditional cyber warfare typically involves digital intrusions into networks or software systems, cyber-physical warfare involves kinetic attacks on infrastructure whose disruption generates effects within digital systems.

In conventional cyber operations, adversaries seek to penetrate networks through malware, intrusion, or exploitation of software vulnerabilities (Rid, 2013; Valeriano & Maness, 2015). By contrast, cyber-physical disruption may occur when physical attacks target infrastructure that underpins digital networks. In such cases, kinetic strikes on data centers, Internet exchange points, or communication infrastructure can generate outcomes similar to cyber-attacks, including service disruption, network outages, and economic losses.

The reported strike affecting infrastructure associated with AWS facilities in the Gulf illustrates this dynamic. Rather than attempting to penetrate cloud systems digitally, the attack reportedly targeted supporting physical infrastructure. Although the resulting disruption was limited, the incident demonstrates how physical attacks on digital strategic nodes can produce cyber-like operational effects.

This dynamic challenges conventional distinctions between cyber operations and traditional military action. As digital infrastructure becomes increasingly central to economic activity, government operations, and communication networks, the disruption of physical infrastructure may generate cascading effects across digital systems.

In this sense, cyber-physical warfare reflects the growing integration of digital networks and physical infrastructure within modern societies. The strategic significance of such infrastructure suggests that future conflicts may increasingly involve attacks on infrastructure nodes that combine high connectivity with high systemic importance.

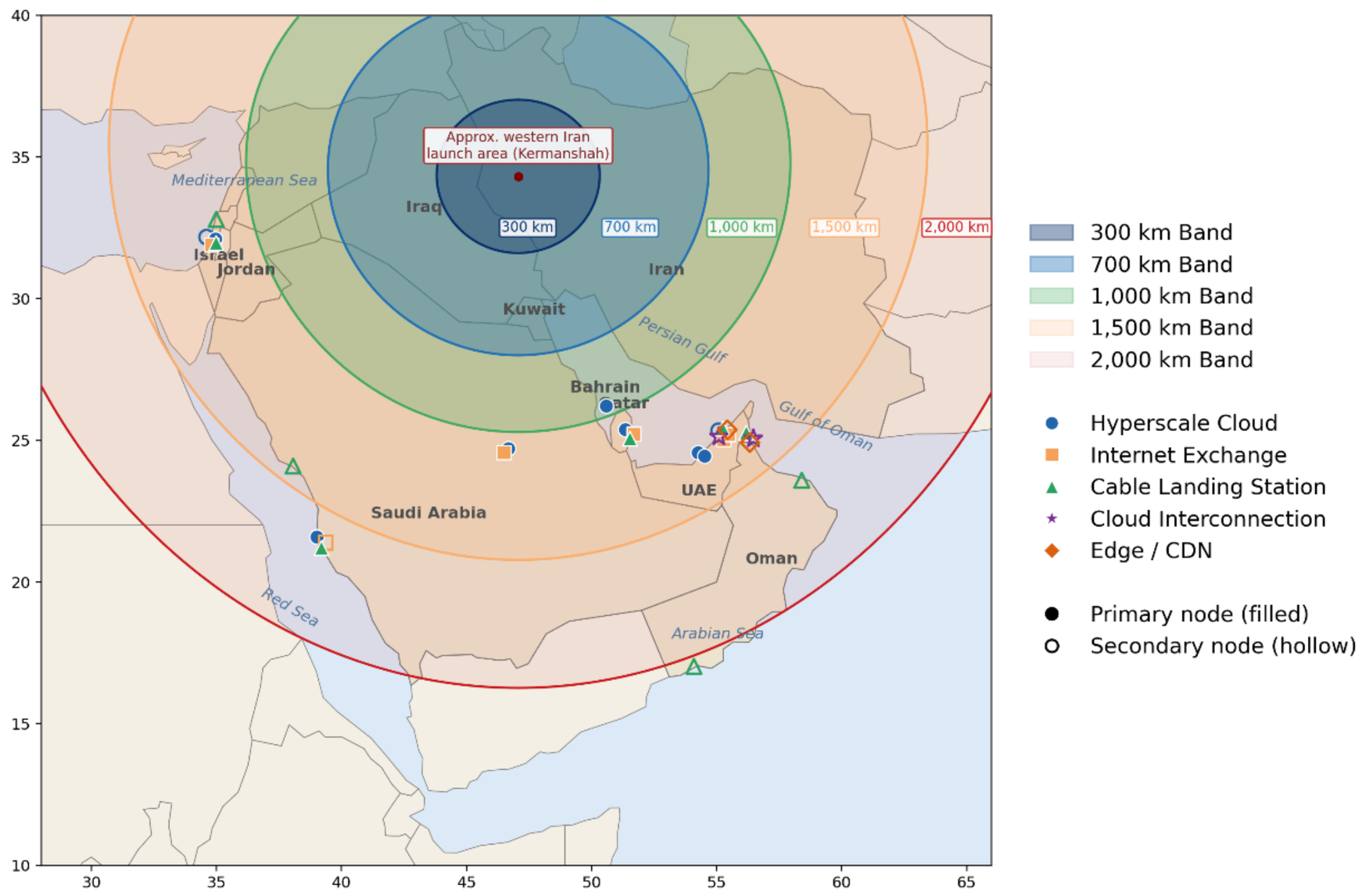

Figure 2. Digital Strategic Nodes Within Layered Iranian Missile Range Bands in the Middle East.

Note: The figure overlays approximate 300 km, 700 km, 1,000 km, 1,500 km, and 2,000 km range bands from western Iran with selected hyperscale cloud infrastructure, Internet exchange points, submarine cable landing stations, cloud interconnection hubs, and edge-distribution nodes across the Middle East. These bands are intended as an analytical visualization of layered reach rather than a precise probability model of strike likelihood. Inner bands indicate comparatively closer and more accessible targets, whereas outer bands denote targets that remain within reach of longer-range missile systems but may require more demanding strike profiles. Mapping regional digital infrastructure in this way suggests an interconnected network of approximately 28 digital strategic nodes, highlighting the geographic overlap between missile reach and concentrated digital infrastructure nodes that exhibit high levels of connectivity and concentration.

Table 1. Digital Strategic Nodes in the Middle East

Node Type	Node Status	Location	Country	Operator / Role	Distance from Iran	Missile Range Band
Hyperscale Cloud	Primary	Bahrain Region	Bahrain	Amazon Web Services	~930 km	1,000 km band
Hyperscale Cloud	Primary	Abu Dhabi	United Arab Emirates	AWS Middle East (UAE) Region	~1,250 km	1,500 km band
Hyperscale Cloud	Primary	Abu Dhabi	United Arab Emirates	Microsoft Azure UAE Central	~1,250 km	1,500 km band
Hyperscale Cloud	Secondary	Dubai	United Arab Emirates	Microsoft Azure UAE North	~1,200 km	1,500 km band
Hyperscale Cloud	Primary	Doha	Qatar	Microsoft Azure Qatar Central	~980 km	1,000 km band
Hyperscale Cloud	Secondary	Tel Aviv	Israel	Microsoft Azure Israel Central	~1,250 km	1,500 km band
Hyperscale Cloud	Primary	Tel Aviv	Israel	Google Cloud Israel Region	~1,250 km	1,500 km band
Hyperscale Cloud	Primary	Jeddah	Saudi Arabia	Oracle Cloud Saudi West	~1,650 km	2,000 km band
Hyperscale Cloud	Primary	Riyadh	Saudi Arabia	Oracle Cloud Saudi Central	~1,350 km	1,500 km band
Internet Exchange	Primary	Dubai	United Arab Emirates	UAE-IX	~1,200 km	1,500 km band
Internet Exchange	Primary	Dubai	United Arab Emirates	DE-CIX Dubai	~1,200 km	1,500 km band
Internet Exchange	Primary	Riyadh	Saudi Arabia	Saudi Internet Exchange	~1,350 km	1,500 km band
Internet Exchange	Secondary	Jeddah	Saudi Arabia	KACIX	~1,650 km	2,000 km band
Internet Exchange	Primary	Doha	Qatar	Qatar Internet Exchange	~980 km	1,000 km band
Internet Exchange	Primary	Tel Aviv	Israel	Israel Internet Exchange	~1,250 km	1,500 km band
Cable Landing Station	Primary	Fujairah	United Arab Emirates	Global submarine cable hub	~1,300 km	1,500 km band
Cable Landing Station	Primary	Dubai	United Arab Emirates	Gulf cable landing station	~1,200 km	1,500 km band
Cable Landing Station	Primary	Jeddah	Saudi Arabia	Red Sea cable hub	~1,650 km	2,000 km band
Cable Landing Station	Secondary	Yanbu	Saudi Arabia	Red Sea landing station	~1,700 km	2,000 km band
Cable Landing Station	Primary	Doha	Qatar	Gulf cable gateway	~980 km	1,000 km band
Cable Landing Station	Secondary	Muscat	Oman	Arabian Sea cable hub	~1,500 km	1,500 km band
Cable Landing Station	Secondary	Salalah	Oman	Global cable landing hub	~1,900 km	2,000 km band
Cable Landing Station	Primary	Tel Aviv	Israel	Mediterranean landing hub	~1,250 km	1,500 km band
Cable Landing Station	Secondary	Haifa	Israel	Mediterranean landing station	~1,270 km	1,500 km band
Cloud Interconnection	Secondary	Dubai	United Arab Emirates	AWS Direct Connect	~1,200 km	1,500 km band
Cloud Interconnection	Secondary	Fujairah	United Arab Emirates	AWS Direct Connect	~1,300 km	1,500 km band
Edge / CDN	Secondary	Dubai	United Arab Emirates	Amazon CloudFront Edge	~1,200 km	1,500 km band
Edge / CDN	Secondary	Fujairah	United Arab Emirates	Amazon CloudFront Edge	~1,300 km	1,500 km band

Note: Distances are approximate great-circle estimates measured from western Iran (near Kermanshah) and rounded to the nearest ten kilometers. Range bands correspond to the layered missile reach visualization presented in **Figure 2**. Primary nodes refer to regional cloud regions, major Internet exchange points, or principal submarine cable landing hubs, whereas secondary nodes represent supplementary interconnection, redundancy, or edge-distribution facilities.

Table 2. Node Distribution by Range Band

Range Band	Number of Nodes
≤1000 km	4
1000–1500 km	19
1500–2000 km	5

Note: Node counts correspond to the expanded inventory presented in **Table 1** and reflect approximate classification based on distance from western Iran (Kermanshah reference point).

7. Implications for Cyber Deterrence and Infrastructure Security

The potential targeting of digital infrastructure carries several important implications for cyber deterrence and the security of critical infrastructure, particularly as cyberspace becomes increasingly integrated into broader national security strategies (Singer & Friedman, 2014).

First, the increasing centralization of cloud infrastructure may generate new forms of systemic vulnerability. Hyperscale data centers improve efficiency by concentrating computing resources and digital services within a limited number of facilities. However, this same concentration may create critical points of failure within digital networks. Disruptions affecting a small number of hyperscale facilities could potentially generate cascading effects across financial systems, logistics networks, and digital services that depend on cloud infrastructure.

Second, the emergence of cyber-physical disruption suggests that cyber deterrence strategies may need to expand beyond traditional network defense. Much of existing cyber security policy focuses on preventing digital intrusions, malware attacks, and network exploitation. However, as digital infrastructure becomes increasingly dependent on physical facilities such as data centers and network exchange hubs, protecting these locations from kinetic attack becomes an essential component of cyber resilience.

Third, the potential militarization of digital infrastructure raises important questions regarding international norms governing the protection of civilian digital systems. Cloud platforms increasingly host government services, financial systems, and civilian communications infrastructure. If hyperscale data centers become viewed as legitimate military targets, the distinction between civilian and military digital infrastructure may become increasingly blurred. This development may generate new challenges for international security and raise questions regarding the legal and normative status of digital infrastructure during armed conflict.

Taken together, these developments suggest that the protection of digital infrastructure may become an increasingly central element of both cyber security strategy and broader national security planning.

Conclusion

The rapid expansion of cloud computing has fundamentally reshaped the strategic architecture of global digital infrastructure. Hyperscale data centers now function as critical nodes supporting economic activity, government services, and technological innovation across national and regional systems. As a result, digital infrastructure has become increasingly central to both economic resilience and national security.

This article has examined how the concentration of cloud infrastructure may generate new forms of strategic vulnerability. The reported targeting of infrastructure associated with AWS facilities during the 2026 U.S.–Iran conflict illustrates how hyperscale data centers may increasingly become integrated into the strategic landscape of modern conflict. When large portions of digital services are concentrated within a limited number of physical facilities, disruptions affecting these locations may produce cascading effects across interconnected digital systems.

To analyze this dynamic, the article introduced the concept of Digital Strategic Nodes, highlighting how infrastructure that combines high levels of connectivity and concentration may acquire disproportionate strategic significance. The mapping of digital infrastructure across the Middle East further demonstrates how many of these nodes fall within the strike range of regional missile systems, creating structural exposure between digital infrastructure and military dynamics.

The emergence of cyber-physical warfare suggests that future conflicts may increasingly involve interactions between digital systems and physical infrastructure. Rather than relying solely on cyber intrusions, actors may seek to disrupt critical digital services through physical attacks on infrastructure nodes that underpin digital networks.

Understanding this evolving dynamic will therefore be essential for policymakers and security practitioners seeking to protect critical infrastructure and maintain stability in the digital age. As digital infrastructure becomes increasingly concentrated within hyperscale facilities and network hubs, strategies for infrastructure protection, redundancy, and resilience will likely become central elements of future national security planning.

Future research should further examine how the architecture of digital infrastructure shapes strategic vulnerability and how international security institutions may adapt to the growing importance of digital systems in modern conflict.

References

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58. https://doi.org/10.1145/1721654.1721672

Associated Press. (2026, March 2). Iranian strikes on Amazon data centers highlight industry's vulnerability to physical disasters. https://apnews.com/article/71066b0a822c4cfd88b61e3fe79af917

Borghard, E. D., & Lonergan, S. W. (2017). The logic of coercion in cyberspace. *Security Studies*, *26*(3), 452–481. https://doi.org/10.1080/09636412.2017.1306396

Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2019). *The business of platforms: Strategy in the age of digital competition, innovation, and power*. Harper Business. https://www.harpercollins.com/products/the-business-of-platforms-michael-a-cusumano-annabelle-gawer-david-b-yoffie

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security, 44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Farrell, H., & Newman, A. L. (2022).*Underground empire: How America weaponized the world economy*. Henry Holt and Company.

Financial Times. (2026, March 6). *Iran hits Amazon data centres in jolt to Gulf AI drive.* https://www.ft.com/content/09fa5c20-2c8f-4f41-9d91-c78476eaac20

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security, 38*(2), 41–73. https://doi.org/10.1162/ISEC_a_00136

Healey, J. (2011). *A fierce domain: Conflict in cyberspace, 1986–2012*. Cyber Conflict Studies Association. https://cyberconflict.org/a-fierce-domain/

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press. https://yalebooks.yale.edu/book/9780300201260/the-virtual-weapon-and-international-order/

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy, 9*(3), 49–51. https://doi.org/10.1109/MSP.2011.67

Lewis, J. A. (2014). *Cybersecurity and critical infrastructure protection*. Center for Strategic and International Studies. https://www.csis.org/analysis/cybersecurity-and-critical-infrastructure-protection

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation. https://www.rand.org/pubs/monographs/MG877.html

Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

Mueller, M. (2017). *Will the Internet fragment? Sovereignty, globalization and cyberspace*. Polity Press. https://www.politybooks.com/bookdetail/?isbn=9781509501250

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Reuters. (2026, March 2). Amazon cloud unit flags issues at Bahrain and UAE data centers amid Iran strikes. https://www.reuters.com/world/middle-east/amazon-cloud-unit-flags-issues-bahrain-uae-data-centers-amid-iran-strikes-2026-03-02/

Rid, T. (2013). *Cyber war will not take place*. Oxford University Press. https://global.oup.com/academic/product/cyber-war-will-not-take-place-9780199338177

Seabrooke, L., & Wigan, D. (2021). The governance of global infrastructure. *Review of International Political Economy*. https://doi.org/10.1080/09692290.2021.1897287

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press. https://global.oup.com/academic/product/cybersecurity-and-cyberwar-9780199918096

Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security, 41*(3), 72–109. https://doi.org/10.1162/ISEC_a_00267

Statista. (2024). *Market share of leading cloud infrastructure service providers worldwide from 2017 to 2024*.

https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/

Synergy Research Group. (2024). *Cloud market share: AWS, Microsoft and Google continue to dominate global cloud infrastructure market*.

https://www.srgresearch.com/articles/aws-microsoft-and-google-continue-to-dominate-cloud-market

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press. https://global.oup.com/academic/product/cyber-war-versus-cyber-realities-9780190204792

Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press. https://global.oup.com/academic/product/cyber-strategy-9780190618094

Varian, H. R. (2019). Artificial intelligence, economics, and industrial organization. *Economics of Innovation and New Technology, 28*(8), 1–12. https://doi.org/10.1080/10438599.2019.1565293