YourLawArticle

Open Access Law Journal, ISSN (O): 3049-0057

Editor-in-Chief – Prof. (Dr.) Amit Kashyap; Publisher – Reet Parihar

Cyber Warfare And Evolving Digital Geopolitics

Authored by:

Adv Kavita N Solunke, (BA, BSL, LLM, GDC&A, PG(ADR), STAR Cyber Crime Intervention Officer, (CCIO), Additional Government Pleader, Arbitrator, Mediator, High Court of Mumbai & Notary Govt of India

&

Dr Rashmi Solunke, M.B.B.S., DNB (Anaesthesia), Aakash Healthcare Super Speciality Hospital, Dwarka, New Delhi

Published on: 27th March 2026

Abstract

Cyber warfare has moved from the margins of defence policy to the centre of contemporary security and statecraft. As states weaponise cyberspace for espionage, disruption and coercive signalling, traditional concepts of sovereignty, deterrence and the law of armed conflict are placed under sustained strain. This paper examines the evolution of cyber warfare, its integration into great-power rivalry and regional conflicts, and the emergence of a distinct "digital geopolitics" in which infrastructure, data and standards become strategic terrain. It then analyses the developing international legal framework, with particular emphasis on the Tallinn Manual project and current debates on sovereignty, due diligence and state responsibility in cyberspace. Finally, it sketches key trends including AI-enabled operations, critical-infrastructure targeting and India's new Joint Doctrine for Cyberspace Operations and outlines policy imperatives for managing escalation and building a more stable cyber order.

Keywords: Cyber warfare, digital geopolitics, cybersecurity, Tallinn Manual, international law, state responsibility, cyber deterrence, India cyber doctrine, critical infrastructure, artificial intelligence

1. Introduction

The digitalization of the economy, the state, and daily life has led to a highly networked world in which cyber operations can produce strategic effects across borders without physical presence or kinetic force.[1] Cyber warfare, broadly defined as the employment of cyber power by state or state-sponsored actors to accomplish strategic or military objectives, has become a major instrument of power.[2] Whether the cyber operations accompanying Russian actions in Ukraine, or the emerging US-China rivalry, digital power has become a supplement to, or at times a substitute for, conventional military power and economic coercion.[3]

At the same time, the global spread of digital infrastructure, platforms, and data flows has also spawned a new level of "digital geopolitics."[4] In this new environment, the management of submarine cables, cloud infrastructure, standards organizations, and data governance structures increasingly recognizes the strategic value of these assets.[5] In this new environment, cyber warfare operations cannot be viewed in isolation; instead, they are shaped by and help shape the broader geopolitical environment.

This paper seeks to position cyber warfare within this new evolving digital geopolitical environment. This paper has three main objectives: to provide an overview of the strategic logic of cyber warfare operations, to examine the emerging legal and normative frameworks, and to explore the future trajectory of cyber warfare, including the implications for India.

2. Conceptualising Cyber Warfare

2.1 Definition and modalities

S&P Global states that cyber warfare is "a series of digital attacks used by one nation state to disrupt, damage or infiltrate the infrastructure of another nation state". Other sources add that

[1] Industrial Cyber, 'Growing Convergence of Geopolitics and Cyber Warfare Continue to Threaten OT and ICS Environments' (17 February 2024).
[2] S&P Global, 'What Is Cyber Warfare?' (27 October 2024).
[3] Reuters, 'Russian Spies Behind Cyber Attack on Ukraine Power Grid in 2022 – Researchers' (9 November 2023).
[4] 'Navigating the Nexus: Geopolitical, International Relations and Digital Studies' (2025).
[5] RANE, 'Cyber Risk Outlook 2025: RANE's 3–5 Year Analysis of Cyberspace in Geopolitics' (14 September 2025).

cyber warfare activities include those which are below the level of "armed attack" but which nevertheless have strategic impact. The modalities of cyber warfare include:

1. **Cyber espionage** – the infiltration of another state's infrastructure for the exfiltration of information of military, diplomatic, or economic interest.

2. **Cyber sabotage** – the disruption or destruction of another state's infrastructure, including industrial control systems and critical infrastructure.

3. **Information and influence operations –** the use of digital platforms to disseminate disinformation, shape public opinion, and create distrust of institutions.[6]

4. **Preparatory operations –** the pre-positioning of malware or access within the infrastructure of another state to enable subsequent cyber warfare options ("left of boom" cyber posturing). The same technical capabilities can be used to accomplish multiple objectives, e.g., the same access gained for espionage can be repurposed for disruption.[7]

2.2 Distinctive features

Cyber warfare is distinct from conventional kinetic warfare in a number of key respects:

- Low entry price and asymmetrical potential: high-end cyber warfare requires expertise and investment, but the price is relatively low, allowing even small or less wealthy nations to gain a disproportionate level of power in the world.

- Attribution difficulties: the technical and operational complexity of cyber warfare, combined with the use of proxies and false flags, makes confident and timely public attribution of cyber attacks difficult and time-consuming.

- Interdependence and spill over effects: cyber attacks on the infrastructure of one state can have spillover effects on the infrastructure of other states, particularly in the realm of the internet and the cloud.

- The blurring of war and peace: cyber warfare is often below the threshold of war, creating a situation of permanent strategic competition, blurring the line between war and peace.

[6] Tixeo, 'Cyberwarfare: Strategies, Threats, and Global Geopolitical Challenges' (2024).
[7] SIT Journal, 'Cyber Warfare and Its Place in Modern Geopolitics and War' (2025).

3. Cyber Warfare in Contemporary Geopolitics

3.1 Russia–Ukraine and hybrid conflict

The Russia-Ukraine conflict is a prime example of the integration of cyber warfare with conventional warfare as part of a hybrid warfare approach. Since at least 2014, Russia has conducted disruptive cyber operations against the government of Ukraine, its media entities, and infrastructure, including power grid compromises by Russian intelligence services. These operations have had the objective of destabilizing the government of Ukraine, shaping public opinion, and advancing broader Russian political and military interests.

It has been observed that operations against operational technology networks, including energy and industrial control systems, have also been used for strategic purposes. The operations against the power grid of Ukraine in 2022 are a prime example of sophisticated malware and coordination with physical operations, highlighting the integration of cyber warfare with conventional warfare.[8]

3.2 Great power cyberpolitics and cyberhegemony

At the systemic level, cyber activities are now integrated into great power rivalry and competition, particularly between the USA and China.[9] This rivalry and competition now encompass:

- Governance: contrasting visions of how to best organize and run cyberspace – an open and multi-stakeholder vision versus sovereignty-centric and state-centric models.
- Technologies: including 5G, cloud computing, artificial intelligence, and semiconductors – where supply chain and standards can create long-term competitive advantage.
- Military intelligence: where there has been a series of cyber espionage and intellectual property theft activities, and efforts to map each other's critical infrastructure.

Recent research in political science suggests that cyber activities promote "expansionist" strategies for great powers to achieve global reach in cyberspace to gain informational advantage and promote norms – and to achieve global "cyberhegemony".

[8] Pepperdine Policy Review, 'A Case Study of Russian Cyber Attacks on the Ukrainian Power Grid' (2024).
[9] Cambridge University Press, 'Great Power Cyberpolitics and Global Cyberhegemony' (2026).

3.3 Non state actors and proxy dynamics

There are increasingly non-state actors involved in cyber warfare, including criminal syndicates, hacktivists, and private contractors. These have complex relationships with states. Industrial control system studies have shown that state-sponsored hacking groups "hand in hand with criminal organizations" can provide plausible deniability and diversified toolsets.

In Ukraine, groups of patriotic hackers have been involved in operations that are sympathetic to state interest. This blurs the lines of international law, which traditionally emphasizes state responsibility.

4. Digital Geopolitics: Infrastructure, Data, and Standards

4.1 Strategic Infrastructure and Supply Chains

While digital geopolitics was once characterized by individual incidents of cyberattacks, it is now increasingly viewed as long-term competition in shaping the digital world. The new strategic priorities in digital geopolitics include:

- The subsea cables, data centers, and satellite constellations that carry much of the world's data and represent potential sources of weakness and power.
- The cloud wars: who controls the major cloud platforms and how this gives access to large volumes of data and facilitates influence operations.
- Supply chain security in areas such as semiconductors and telecommunications, as states attempt to reduce geopolitical risks by 'reshoring' or 'friend-shoring' critical supply chain infrastructure.[10]

Analysts argue that there is an increased risk of feedback loops in geopolitics as sanctions and export controls contribute to an increased risk of cyber threats due to supply chain fragmentation.

4.2 Standards, norms, and governance models

Another area where the stakes are being played out in the digital geopolitics arena is the control of technical standards and the governance forums. Countries and coalitions are competing in

[10] Getronics, 'When Geopolitics Becomes a Security Gap' (2025).

standard setting organisations and internet governance debates to ensure the preferences of nations are incorporated into the global technology landscape on issues such as security, interoperability, encryption, and surveillance.

There are emerging competing visions of digital sovereignty, with some countries advocating for data localisation, robust state control, and the screening of online platforms for national security, while others are advocating for the free flow of data across borders. These differences will have implications for the legal and technical landscape in which cyber operations take place.

5. International Law and Normative Frameworks

5.1 The Tallinn Manual project

One of the most important attempts to clarify how existing international laws apply in cyberspace is the Tallinn Manual project, initiated by the NATO Cooperative Cyber Defence Centre of Excellence.[11] The first edition of the Tallinn Manual on the International Law Applicable to Cyber Warfare (2013) establishes ninety five "black letter rules" of international law in the areas of jus ad bellum, international humanitarian law, sovereignty, state responsibility, and neutrality in the context of cyber conflicts that attain the intensity of armed conflict.[12]

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017) extends its scope to cover various types of hostile cyber operations below the armed conflict threshold by establishing 154 rules of international law in various areas such as human rights law, air law, space law, and the law of the sea. While these two manuals do not represent binding rules of international law, they reflect the consensus and divergent views of experts who worked together in these projects and are now widely regarded as important references in the field.

5.2 Sovereignty, due diligence and state responsibility

The major debate here is on the violation of the principle of state sovereignty through cyber operations. Some countries, like the European countries, have the view that if cyber operations are not consensual and are conducted remotely, then the operations can violate the principle of

[11] NATO Cooperative Cyber Defence Centre of Excellence, 'The Tallinn Manual'.
[12] Georgetown Law Library, 'Tallinn Manual & Primary Law Applicable to Cyber Conflicts' (2015).

sovereignty, despite the operations not being the use of force. Other countries have the different view that the operations should cause physical damage or loss of functionality in the targeted state in order to violate the principle of sovereignty.

Relatedly, the principle of due diligence, which has long been recognized in the context of environmental and transboundary harm, is now being referred to in the context of cyber. The issue is whether there is a legal duty for states to ensure that reasonable steps are taken to prevent their territory or infrastructure being used to engage in cyber activities that cause serious harm to other states, and how this principle is engaged in the context of non-state and proxy actor involvement. The Tallinn 2.0 commentary recognizes the principle of due diligence but notes that state practice is divided.

The rules of state responsibility are also engaged in the context of cyber. This is because if a state can be said to be involved in cyber activities – for example, if it has effective control over non-state actors or if state organs are directly involved – this can give rise to a duty to make reparation and/or to engage in countermeasures.

5.3 UN processes and voluntary norms

Aside from the expert projects, the UN has also established parallel processes, the GGE and OEWG, which have resulted in the establishment of voluntary norms of responsible state conduct in cyberspace. Among these are the undertakings not to attack critical infrastructure used for the delivery of services to the public during peacetime, to assist other states in dealing with ICT incidents, and to combat cybercrime.

However, it has to be noted that such norms are voluntary and are based on political, not legal, undertakings. The geopolitical nature of the issues has hindered the establishment of binding instruments, with some states disagreeing on what conducts are deemed unacceptable and how they are to be measured.

6. India, Cyber Warfare, and Digital Geopolitics

6.1 India's strategic posture and institutional architecture

The digitalisation of India and its regional strategic environment have made cyber security and cyber warfare central to India's strategic thinking. [13] Over the past ten years, India has

[13] CENJOWS, 'Indian Cyberspace: Threat Prevention' (2024).

developed critical institutions, including the National Critical Information Infrastructure Protection Centre (NCIIPC), the Indian Computer Emergency Response Team (CERT In), and cyber cells in the Indian armed forces.

In 2024-25, India promulgated its first Joint Doctrine for Cyberspace Operations (JDCO), which is intended to provide a common framework for planning and executing cyber operations by the Indian tri services. [14] The commentary to the doctrine asserts that the doctrine aspires to fuse the capabilities of the Indian military for defence and offence in land, air, sea, and space domains to "retain its own freedom of action and deny the adversary's freedom of action in the cyber domain," while also considering cyberattacks to support conventional attacks as the equivalent of the latter against India.[15] The doctrine places a strong emphasis on the demonstration of capabilities for defence and offence in the cyber domain. [61]

Analysts argue that JDCO marks a significant step in centralising and formalising India's cyber-military posture, supporting jointness among the services and aligning with broader processes of theatre-command integration. [16]

Cyber operations in South Asia must be understood against the backdrop of long-standing India-Pakistan and India -China tensions.

6.2 Regional dynamics and crisis stability in South Asia

and parallel developments in neighboring states could have implications for crisis stability, especially in relation to the use of cyber for probing, disrupting, and signaling during military stand-offs.

An important concern is that cyberattacks on critical infrastructure and/or military networks during a crisis situation, which are intended, misattributed, or mistaken, could be perceived as escalatory and/or indicative of preparations for further kinetic actions, thus accelerating decision-making timelines and heightening the prospect of miscalculations. The clear declaration that cyberattacks launched in support of conventional attacks can be considered to be armed attacks only serves to heighten this concern. On the other hand, robust cyber defenses and declaratory policies can be useful for deterrence and crisis stability if articulated and presented clearly.

[14] Press Information Bureau, 'Joint Doctrines for Cyberspace Operations & Amphibious Operations' (6 August 2025).
[15] CISS, 'India's Joint Doctrine for Cyberspace Operations' (2025).
[16] Vajiram & Ravi, 'India's First Joint Doctrine for Cyberspace Operations' (2025).

6.3 India in global digital geopolitics

India is also a growing player in global digital geopolitics. The Digital India programme, data governance debates, and the country's participation in chip and 5G supply chain partnerships reflect its status as a large digital marketplace and a normative power.

On the one hand, India has taken a strong stand on the issue of data localisation for certain categories of data and its vision of digital sovereignty, while on the other, it has been a part of the deliberations of the cyber security, critical infrastructure protection, and trusted supply chains discussions of the 'like-minded' nations.

The balance between its strategic autonomy and its participation in the emerging digital alliances will be critical to its cyber geopolitical footprint in the coming decade.

7. Emerging Trends and Future Trajectories

7.1 AI enabled cyber and information operations

The fusion of artificial intelligence with cyber warfare and information operations is a notable emerging trend. Cybersecurity assessments of the industrial sector highlight the role of artificial intelligence and machine learning in increasing the level of sophistication of cyber operations targeting critical infrastructure, including the discovery of vulnerabilities and the adaptation of malware. At the same time, artificial intelligence can play a role in the detection of anomalies and the response to cyber threats.

In the information domain, the emergence of generative artificial intelligence enables the creation of believable deepfakes and disinformation, which can have implications for the integrity of elections and the cohesion of societies. This emerging trend implies that "cognitive security," or the protection of societies' decision-making processes, will become as important as protecting societies' networks and devices.

7.2 Critical infrastructure targeting and OT security

Cyberattacks on operational technology (OT) and industrial control systems (ICS) in sectors such as power grids and pipelines, and health facilities, are on the rise and becoming increasingly sophisticated. Experts have emphasized that threat actors are now targeting supply chain risks and leveraging ransomware and data exfiltration for exerting political pressure.

These environments used to be air-gapped and now are increasingly connected to IT networks and the internet.

The Russia-Ukraine conflict and other incidents in different parts of the world have underscored the cross-border effects of OT cyberattacks and the resultant complex issues of proportionality and responsibility under international law. For countries like India, where there is an exponential growth in digital infrastructure and varying levels of cyber maturity in different sectors, OT security is emerging as a critical area of strategic interest.

7.3 Fragmentation, blocs and "multi polar" cyberspace

Lastly, there are predictions of a more fragmented, "multi polar" cyberspace where groups of nations are likely to form "like-minded" blocs based on common values, norms, and supply chains. According to RANE's medium-term analysis, geopolitical tensions are likely to continue being the main influencer of cyber risk over the next three to five years, with significant cyber incidents mirroring tensions between great powers. This fragmentation may help alleviate some of the dependencies between nations but may also result in the creation of incompatible norms, duplicated infrastructure, and increased barriers to cooperation, especially when dealing with cybercrime. The challenge facing international law and diplomacy will be to ensure that enough interoperability and common norms are maintained to avoid escalation, despite the divergent paths being taken by nations towards digital sovereignty.

8. Conclusion

Cyber warfare has evolved to the point that it has become an integral component of statecraft and military strategy, and is inextricably linked with broader concepts of digital geopolitics. Cyber warfare leverages the interconnectedness of the internet and other digital technologies to achieve strategic objectives at relatively low cost, but also poses serious challenges in attribution, deterrence, and legal control. The ongoing conflict between Russia and Ukraine, the cyber rivalry between the United States and China, and the string of major cyber attacks underscore the reality that cyberspace has become the primary site of geopolitical contest, not the secondary site that it once was.

However, international law has begun to adjust, with the Tallinn Manuals offering an advanced interpretive framework, and the UN processes establishing voluntary norms of responsible conduct. Nevertheless, there are considerable doctrinal uncertainties, particularly with respect

to sovereignty, due diligence, and the approach to the armed attack threshold. The militarisation of cyber space and the integration of AI and OT targeting also increase systemic risks.

For India, and for states more generally, the imperative is twofold. It is to develop robust cyber capabilities and doctrines, such as the Joint Doctrine for Cyberspace Operations, but also to contribute to the development of norms, transparency, and conflict management tools to mitigate the risks of escalation. Will the geopolitics of the digital world develop into a relatively ordered world, governed by rules, or will it increasingly become an ungoverned world of disruptive competition? The answer will depend on the choices made in the coming decade.