Cybersecurity and Geopolitical Transformation across Eurasia and the Indo-Pacific

Power, Strategy, and Technology in the Cyber Domain

Across Eurasia and the Indo-Pacific, cybersecurity challenges are increasingly linked to broader transformations in regional and global order. As a result, this interconnected vast space has become an important arena of geopolitical competition, technological change, and security reconfiguration. Although Eurasia and the Indo-Pacific are often treated as separate geopolitical regions, in reality they are deeply connected through trade routes, digital and energy networks, submarine cables, technological supply chains and critical resources. Cybersecurity challenges, such as attacks on critical infrastructure or disruptions of supply chains, in one region can produce effects across the other. This growing interdependence makes Eurasia and the Indo-Pacific a shared space characterized by the increasing centrality of cybersecurity in geopolitical competition, the emergence of new forms of cyber statecraft and the diffusion of cyber capabilities among states and non-state actors.

As states across this space are increasing their reliance on digital infrastructure, cloud technologies, artificial intelligence, data flows, and networked platforms, they face both similar opportunities and shared vulnerabilities. Cyberspace brings significant opportunities by creating potential for economic development, technological connectivity and international cooperation. At the same time, it also brings vulnerabilities arising from growing digital interdependence and the increasing reliance of states on critical infrastructures and technologies owned by private corporations.

In addition, some other categories of non-state actors, such as proxy movements, hacktivist groups, criminal networks and cyber militias, are playing an increasingly important role in cyberspace. Very often they are operating across national borders and outside established frameworks of attribution and accountability, but they are increasingly capable of conducting disruptive activities, influencing information environments, and participating in geopolitical competition.

In this context, states find themselves operating alongside, competing with, and at times fighting against a diverse range of non-state actors that have a growing role in shaping, controlling or disrupting the digital environment. One direct consequence is that technological, informational, and security dimensions become deeply interlinked and states must balance the pursuit of innovation, connectivity and technological openness with the need to maintain strategic autonomy, protect critical systems and manage new forms of dependency.

Recent crises and conflicts have further demonstrated that small vulnerabilities in digital ecosystems can have implications that extend far beyond the technical domain. They have shown not only the emergence of cyber threats targeting critical infrastructure and information systems, but also the rise of cyber-enabled forms of confrontation that produce less visible, but equally important effects, such as shaping information environment, influencing public perceptions and undermining public trust.

Such evolutions show that technological innovation can serve both constructive and disruptive purposes. They also indicate that cybersecurity has evolved from a technical issue into an essential concern for national security, state capacity, economic stability and societal cohesion. All these developments, coupled with the decline of unipolarity and the emergence of a more multicentric global order, call for a deep reflection about how power and authority are exercised and contested in cyberspace and how traditional understandings of sovereignty, security, deterrence are changing. They also raise significant questions of how and with what implications the boundaries between peace and conflict, defence and offense, civilian and military, public and private domains are becoming blurred.

This call for papers invites original, unpublished empirical, theoretical, and policy-oriented contributions that examine how cyberspace and emerging technologies are transforming geopolitical relations, security practices, regional security architectures and strategic competition across Eurasia and the Indo-Pacific. We particularly welcome contributions addressing cybersecurity, cyber statecraft, cyber capabilities,

cyber-enabled operations, cognitive warfare, technological competition, digital dependencies, and the civil-military applications and implications of emerging technologies. We invite scholars and practitioners from diverse disciplinary backgrounds and we strongly encourage contributions drawing lessons from recent crises and conflicts, concrete case-studies and interdisciplinary approaches.

Contributions may address, but are not limited to, the following six themes:

- Authority, Sovereignty, and Digital Infrastructure
- National Cyber Policies and Regional Cyber Cooperation
- Cyber Statecraft and Strategic Competition
- Cyber-Enabled Operations, Non-State Actors and Hybrid Threats
- Cyber Defence, Deterrence and Critical Infrastructure Protection
- Emerging Technologies and Military Transformation.

Prospective contributors are invited to submit an abstract of up to 300 words outlining the research question, theoretical framework, methodology, and significance of the proposed paper. Abstracts should be accompanied by the author's institutional affiliation, contact details and a short bio (under 100 words).

Abstract submission deadline: 17 August 2026
Abstracts should be sent to Laura-Anca Parepa at: lparepa@mail.doshisha.ac.jp
Notification of review results: 30 August 2026
Final chapters of 8,000- 9,000 words, all inclusive, should be submitted by: 28 February 2027

Accepted chapters will be considered for inclusion in a volume planned for the *Routledge Research in Eurasian Geopolitics* series.

Further details regarding style, requirements and submission procedures will be provided to accepted contributors.