Call for Papers

Studying Cyber Conflict in a Fractured Digital Order: Concepts, Methods, and Evidence

Workshop Convenors:

Jacopo Franceschini jacopofranceschini5@gmail.com

Ayhan Gücüyener Evren ayhangucuyener@hotmail.com

With the "digitalization of everything", scenarios that once sounded dystopian, nationwide blackouts, hospital shutdowns, or supply-chain paralysis triggered by cyber operations, are no longer far-fetched. As digital dependencies deepen, cybersecurity has moved from "computer security" into the realm of high politics: states increasingly treat cyberspace as a domain of competition, and cyber activity now accompanies (and sometimes substitutes for) kinetic force in wider contestation. Yet core concepts remain contested: debates over whether "cyber war" is a useful category, how to conceptualise coercion and deterrence, and what counts as meaningful harm or escalation continue to shape the field.

This workshop asks how we should navigate these conceptual and methodological debates. Put differently, what should we study in cyber conflict, and how should we study it? We focus on the evolution of cyber conflict research and explore how approaches have shifted, what themes have emerged, and which methodological paths are available to researchers.

To advance these questions, the workshop explores interlocking themes. Foundations: Analytical and Critical Approaches to Key Concepts and Methods of Cyber Conflict revisits how notions such as cyber war, coercion, deterrence, escalation, harm, and cyber power translate from traditional security thinking into digital settings. Cyber Diplomacy in a Fractured International Order examines norm-making, confidence-building and professional practice, including UN processes, OSCE measures and regional initiatives. Infrastructures, Breakdown, and Survival Struggles analyses operations against energy, health, logistics and other essential systems and the politics of resilience and recovery. Private Power and Big Tech in Cybersecurity Governance focuses on how platforms, vendors, and security providers shape threat knowledge, incident response, and accountability. Emerging Technologies and Future Trajectories of Cyber Conflict considers how AI/ML, automation and quantum computing reconfigure both conflict dynamics and research agendas; Human Centred Cyber Conflict: Lived Experiences, Agency, and Vulnerability is welcomed as one empirical window among others.

We invite theoretical, conceptual, and empirical papers from junior and senior scholars, including interdisciplinary work across international relations, security studies, science and technology studies, law, and related fields. Example questions include: How should we refine core concepts to capture digital contestation without conceptual overstretch? Under what conditions do cyber operations produce coercive leverage or affect escalation? How are diplomatic and governance efforts pursuing stability amid rivalry and uneven regional priorities? How do infrastructures, private actors, and emerging technologies reshape vulnerability, resilience, and accountability? Papers may use qualitative, quantitative, mixed-method, or interdisciplinary designs. For workshop-related questions, please contact the convenors.