**Critical cybersecurity studies: Perspectives, positionalities, and pathways**

Workshop proposal for ‘The Interconnected Worlds of the Past and the Present: Co-constituting the International’, 9th European Workshops in International Studies, Thessaloniki, 6-9 July 2022

*Tobias Liebetrau, Sciences Po Paris and Danish Institute for International Studies. E-mail: toli@diss.dk*

*Linda Monsees, Institute of International Relations, Prague. E-mail: monsees@iir.cz*

Cybersecurity is core to contemporary scholarly and societal security debate. Critical security studies has left its mark on this debate. A first wave of scholarship challenged positivist assumptions and policy problem driven research agendas by examining the discursive framing of cybersecurity and the use of metaphors and analogies (Betz and Stevens 2013; Cavelty 2013; Hansen and Nissenbaum 2009). In recent years, scholars have introduced Actor-Network-Theory (Balzacq and Cavelty 2016), Sciences and Technology Studies (Liebetrau and Christensen 2021), assemblage theory (Stevens 2020) and computational grammar (Dwyer 2021) to study how cybersecurity is enacted in entanglements of security, politics, and technology. Yet, the field of critical cybersecurity studies needs to continuously be reflective about its own knowledge production (Stevens 2018). Due to the surge in critical cyber security scholarship, we find that is timely to reflect on critical cybersecurity studies’ current perspectives and positionalities to formulate pathways for future scholarship. This concerns its methodologies and theories, as well as its position within an expanding field of critical security studies, on the one hand, and public policy one the other.

How is critical cybersecurity studies affected by and coping with the field of cybersecurity knowledge production being embedded in a world of policy makers, intelligence services, private companies, think tanks and activists? What is the relationship between critical cybersecurity studies and quickly evolving digital technologies? Is critical cybersecurity studies suffering from Western, gendered, or other biases, and how can it be refocused? Should theoretical reflection move closer to or be further distanced from day-to-day cybersecurity events and technological advances? What is specific to critical theory building and knowledge production in the field of cybersecurity?

This workshop invites scholars to reflect on these and related questions. We aim for the workshop to connect scholars that work on these questions across contexts and countries, ideally leading to future projects such as a common publication. We encourage scholars to present research on or related to the following issues

* Knowing and theorizing critical cybersecurity
* Neocolonial dynamics in cybersecurity
* Feminist perspectives on cybersecurity
* The history of cybersecurity research
* Cybersecurity and emerging digital technologies
* Future imaginaries of cyberpeace

**Bibliography**

Balzacq, T., & Cavelty, M. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, 1(2), 176-198.

Betz, David J. and Stevens T. (2013). Analogical reasoning and cyber security, *Security Dialogue*, 44(2), 147–64.

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse, *International Studies Review*, Volume 15: 1, 105–122.

Dwyer, Andrew. (2021). Cybersecurity’s grammars: A more- than- human geopolitics of Computation. *Area.* Special Section, 1-8.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53(4), 1155–1175

Liebetrau, T., & Christensen, K. (2021). The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces. *European Journal of International Security*, 6(1), 25-43

Stevens, C. (2020). Assembling cybersecurity: The politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy,* 41(1), 129–152.

Stevens, T. (2018). Global Cybersecurity: New Directions in Theory and Methods. *Politics and Governance* 6(2), 1-4.