Pre-ECIS SIGSEC Workshop on Cybersecurity, Privacy, and Infrastructures

June 13, 2023 @Kristiansand, Norway

https://ecis2023.no/

Important dates:

- Paper submission deadline: April 16, 2023
- Notification of acceptance: April 30, 2023
- Workshop date: June 13, 2023

Call for Papers

Infrastructures are key to the functioning of any contemporary society and organization, but they are also key for the protection of those societies and organizations. While some infrastructures are more critical than others, they all are inherently vulnerable and exposed to cyberattacks. Further, while some of the infrastructures are built for functionality and effectiveness, some of them are built specifically for security.

Information systems has a long history of infrastructure studies (e.g., Star & Ruhleder, 1996). What has largely been missed from these discussions is security. For instance, in a research agenda for infrastructure studies, security is hardly mentioned (Tilson et al., 2010). Are concerns of security and privacy so indifferent for the development and evolution of infrastructures that they deserve to fade in the background? Clearly not. One can hardly understand the development of Internet and its current materialization without reference to security. The once ideological goal of an open space for unbounded sharing of information has become a fragmented space of isolated small islands surrounded by firewalls and intrusion prevention systems to keep the "enemy at the gates" (Whitman, 2003). Further, advancements in security technologies have contributed importantly to the development of new forms of infrastructures such as decentralized marketplaces.

Some infrastructures are built for security. These security infrastructures are socio-technical and material assemblages that seek to protect and control individuals, organizations, and societies, e.g., as materialized in collectives of organizational policies, technological fabric, and normative structures. Thus, they are not merely technological but also social which is crucial as "overly technological accounts of infrastructure fail to highlight the consequences of technology for data privacy and security" (Parmiggiani & Grisot, 2019). These infrastructures are often reifications of standardized "best practices" that prescribe measures as components of the infrastructures they constitute, and that inscribe behaviour within these infrastructures (Hanseth & Monteiro, 1997). The wide adoption of the standardized practices has meant that those who are touched and controlled by the security infrastructures are many. Consequently, their development, implementation, and evolution concern a much broader audience than the rather marginal groups of niche experts responsible for their implementation. Further, the same technologies that afford security infrastructures can also be exploited for malicious purposes, e.g., to sell illegal goods (Spagnoletti et al., 2022), to create massive-scale botnets for coordinated and targeted attacks against individuals, organizations, and even some of the most powerful societies. They empower individuals and groups with unprecedented force to cause havoc on a large scale.

Several prominent Norwegian IS scholars have spearheaded discussions and research, especially on information infrastructures (e.g., Hanseth, Monteiro, Bygstad, Aanestad). Given the Norwegian context of this year's ECIS, we invite scholars to engage with the intersection of information infrastructures and cybersecurity to provide empirical and conceptual accounts that develop fresh ideas, new perspectives, concepts, and theories that can progress our understanding of cybersecurity, privacy, and infrastructures. In addition, we welcome other related studies dealing with more traditional IS security (e.g, security behaviour, policy compliance) and privacy topics.

The topics for the workshop include but are not limited to:

- Implications of cybersecurity for infrastructure development, implementation, and evolution.
- Designing and implementing security and privacy of infrastructures
- Dynamics of security infrastructures, e.g., what are the generative forces of security infrastructures; how security infrastructures establish governance, control, and discipline.
- How security standards and standardization proliferate through infrastructuring
- Vulnerabilities and resilience of infrastructures.
- Socio-technical conceptualizations of security infrastructures
- Continuity and resilience of infrastructures
- Critical perspectives on cybersecurity and the implications of security infrastructures for individuals, organizations, and societies
- Controlling security behavior and privacy (e.g., policy compliance, privacy by design)

Paper submissions:

Prospective authors are requested to submit their work directly to the workshop chairs via email to sigsec@ecis2023.no. All submissions will be evaluated by the workshop chairs for their topical relevance and quality. Authors attending to the workshop are expected to serve as discussants for other research (more information will follow acceptance).

We invite the following types of submissions:

- *Full paper drafts*: These submissions are close to finished research up to 5000 words (but can be less). Authors submitting full paper drafts are expected to serve as discussants for another article of this submission type.
- *Extended abstracts*: These submissions can present an idea or research-in-progress that is up to 1500 words. Authors submitting extended abstracts are expected to serve as discussants for another article of this submission type.

Registration:

Workshop registration is handled through ECIS online registration system. Please, see ECIS 2023 website for more information (https://ecis2023.no/). We welcome both authors and others interested in the topic to join the workshop.

Workshop format:

This workshop is a paper/idea development workshop. The workshop will include keynotes and roundtable discussions. The discussions will be organized around thematically grouped roundtables. Authors who have submitted their work to the workshop are expected to act as discussants for other participants in the same roundtable. Each paper will get 45min time for discussion.

Keynotes:

Keynotes will be announced later.

Questions:

Should you have any questions related to the workshop, please, contact the chairs (sigsec@ecis2023.no).

Schedule and location:

The workshop will be organized as a full day event on June 13, 2023 in Kristiansand, Norway. Detailed schedule and exact location will be made available prior to the workshop.

Chairs:

Marko Niemimaa (marko.niemimaa@uia.no), University of Agder

Paolo Spagnoletti (pspagnoletti@luiss.it), Luiss University

Jonna Järveläinen (jonna.jarvelainen@utu.fi), University of Turku

Wael Soliman (wael.soliman@uia.no.fi), University of Agder

Mikko Siponen (mikko.t.siponen@jyu.fi), University of Jyvaskyla

Obi Ogbanufe (obi.ogbanufe@unt.edu), University of North Texas

References:

Hanseth, O., & Monteiro, E. (1997). Inscribing Behaviour in Information Infrastructure Standards. *Accounting, Management and Information Technologies*, *7*(4), 183–211.

Parmiggiani, E., & Grisot, M. (2019). DATA INFRASTRUCTURES IN THE PUBLIC SECTOR: A CRITICAL RESEARCH AGENDA ROOTED IN SCANDINAVIAN IS RESEARCH. *Scandinavian Conference on Information Systems*, 1–16.

Spagnoletti, P., Ceci, F., & Bygstad, B. (2022). Online Black-Markets: An Investigation of a Digital Infrastructure in the Dark. *Information Systems Frontiers*, *24*, 1811–1826. https://doi.org/10.1007/s10796-021-10187-9/Published

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research*, *7*(1), 111–134. http://pubsonline.informs.org/doi/abs/10.1287/isre.7.1.111

Tilson, D., Lyytinen, K., & Sørensen, C. (2010). Research Commentary: Digital infrastructures: The missing IS research agenda. *Information Systems Research*, *21*(4), 748–759. https://doi.org/10.1287/isre.1100.0318

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM*, *46*(8), 91–95.