T15P04 / Constructing and defending AI sovereignty in the context of cybersecurity strategy

Topic : T15 / SCIENCE AND TECHNOLOGY POLICY

Chair : Mergen Dyussenov (Astana IT University)

Second Chair : Jen Dodgson (LKY School of Public Policy, National University of Singapore)

GENERAL OBJECTIVES, RESEARCH QUESTIONS AND SCIENTIFIC RELEVANCE

Large-scaleAI models are rapidly seeping into all facets of our lives: whether they are feeding us content on Youtube, suggesting purchases on Amazon or even – in the case of LLMs such as GPT and Claude – replacing search engines as our major source of information. While the base models are mere statistical processes, the consumer-facing elements are carefully fine-tuned and guardrailed to present specific visions of the world. Deepseek is told to avoid answering questions considered politically sensitive in China, while Gemini inserts a distinctly US-centric vision of diversity, equity and inclusion (DEI) into its responses. Already we have seen controversies over potential pro-Chinese manipulation of Tiktok's US content recommendation algorithms, and fierce debates over how governments are to regulate model development and implementation in the US, EU and China. Adding to this difficulty is the inherent uncertainty surrounding the technology: the emergent nature of AI outputs means that predicting model behaviour and data encoding will always be extremely difficult, and every new foundation model is effectively a new parallel world requiring exploration.

This panel will consider how – and indeed if – governments can maintain AI sovereignty in an increasingly borderless world. In doing so, AI sovereignty is analysed in terms of implications for cybersecurity strategy and digital governance. As closed-source black-box AI models increasingly exert their influence on what constitutes 'truth', their owners will have never-before-encountered powers to manipulate the public consciousness across the world. Faced with such a challenge, smaller states must decide how they are to maintain independence in terms of cybersecurity regulation and strategy, particularly when faced with intense pressure from other states. The consequences of this choice do not just affect information security, but also have economic, diplomatic and even – potentially - military consequences. Cybersecurity regulatory approaches risk impeding local technological competitiveness and creating unemployment as workers fail to keep up with current innovations, while locally-focused models struggle to keep up with the capacities of the tech giants. In the present panel we consider how smaller powers can adapt to a world increasingly dominated by AI.

CALL FOR PAPERS

We invite papers exploring the intersection of an emerging concept of AI sovereignty and cybersecurity strategy analysis, as well as its implications for smaller states striving to maintain independence in a world dominated by powerful tech giants and their advanced AI models. As artificial intelligence increasingly shapes media, economies, and social interactions, smaller nations face distinct challenges in safeguarding their informational sovereignty, cultural values, and economic autonomy.

This panel seeks insights into how smaller states can design cybersecurity regulatory frameworks in the broader realm of digital governance that protect local interests without stifling innovation, risking unemployment or succumbing to the pressures of larger, technology-exporting nations. What strategies are available for nations that wish to harness AI for their own growth while ensuring that foreign interests do not disproportionately influence their societies? Topics of interest include the design of national AI policies with implications for national cybersecurity strategy, ethical considerations in localized AI deployment, and approaches to developing domestic AI capabilities that remain competitive yet culturally aligned.

We welcome interdisciplinary submissions that address digital governance, cybersecurity policy, law, technology, and social impact. This discussion aims to build understanding and offer actionable insights into how smaller states can assert agency in an interconnected, AI-driven world, promoting resilience in the face of rapidly evolving cyber threats and related risks.

Specific topics include, but are not limited to:

Cybersecurity Frameworks for Localized AI: Strategies for building robust, adaptive cybersecurity policies tailored to AI systems while considering unique regional and cultural values.

Digital Governance Frameworks and Mechanisms: National AI governance frameworks for creating AI policies that align with national interests, values, and cultural priorities.

Regulatory Approaches to AI Sovereignty: Comparing different models of AI regulation that enable innovation without exposing countries to undue foreign influence.

AI for Economic Resilience in Small States: Investigating how AI can be utilized to strengthen economic independence, diversify industries, and reduce reliance on external digital services.

Case Studies of Small-State Cybersecurity and AI Successes: Analyses of successful frameworks or policies from smaller nations that could serve as models for others.

Cyber Threats in the Context of AI-Driven Influence: How smaller states can protect against AI-enhanced misinformation and disinformation campaigns targeting their populace.

Cybersecurity Policy Analysis Through Stages: Digital agenda-setting, decision-making, implementation, and digital policy evaluation processes.

Papers should be limited to around 6,000 – 8,000 words, including references using the APA style format.