P11 / Cybersecurity: policymaking and institutionalization

Topic : SCIENCE, INTERNET AND TECHNOLOGY POLICY

Chair : Mauro Santaniello (Università degli Studi di Salerno)

Second Chair : Jonathan Kamkhaji (European University Institute)

Third Chair : Giancarlo Vecchi (Politecnico di Milano)

Fourth Chair : Francesco Amoretti (Università degli Studi di Salerno)

GENERAL OBJECTIVES, RESEARCH QUESTIONS AND SCIENTIFIC RELEVANCE

Cybersecurity has become the main digital-related public concern in contemporary societies. The issue has rapidly scaled up the political agenda of international organizations, national governments and local authorities alike, gaining a stable position among the top-level priorities of governments and agencies. Further, the pandemic has boosted the digital transformation all over the world, and sharpened the complexity, the scale, the scope, and the interdependencies of cybersecurity problems. Facing these new collective problems, private and public policies have increasingly been developed in different societal contexts and on multiple institutional levels. A fast-growing branch of policy studies is emerging to better understand these processes of policy-making, and to analyze their impact and consequences on individuals, businesses, public administrations and institutions.

Some scholars have studied how public discourse on cyber security affects the emergence of specific institutional design and policy instruments (Lawson and Middleton 2019; Miao, Xu, Zhu 2019; Stevens 2018). Others have investigated the conditions that enable or prevent policy change in national cybersecurity arenas (Schively 2021). Other studies have adopted a comparative perspective, aiming at identifying economic, cultural, legal and institutional factors that shape different national approaches to cybersecurity policies (Karatas 2020, Shackelford 2021; Creese, Dutton,Esteve-González 2021). Further lines of research have focused on cybersecurity as a matter of international cooperation, both in terms of capacity building and policy transfer (Homburger 2019), and as a field of intergovernmental partnership and foreign policy (Christou 2017; Christou, Lee 2021).

The main objective of this panel is to understand how cybersecurity is getting institutionalized in multilevel, polycentric systems of governance. It aims at convening scholars who are addressing cybersecurity policies from different angles, in order to trigger a discussion about if and how cybersecurity is emerging as a specific domain of public policy.

Papers will present new theoretical and methodological reflections, as well as empirical research, on the institutionalization of cybersecurity and the related processes of policy-making. Presentations will share new analytical frameworks, comparative analyses and in-depth case studies on policy discourses, frames, networks, instruments and outcomes. The panel will take place on-site In Toronto, though allowing remote presentations.

CALL FOR PAPERS

Cybersecurity has become the main digital-related public concern in contemporary societies. The issue has rapidly scaled up the political agenda of international organizations, national governments and local authorities, gaining a stable position among the top-level priorities of governmental institutions. Further, the pandemic has boosted the digital transformation all over the world, and sharpened the complexity, the scale, the scope, and the interdependencies of cybersecurity problems. Facing these new collective problems, private and public policies have increasingly been developed in different societal contexts and on multiple institutional levels. A fast-growing branch of policy studies is emerging to better understand these processes of policy-making, and to analyze their impact and consequences on individuals, businesses, public administrations and institutions.

The main objective of this panel is to understand how cybersecurity is getting institutionalized in multilevel, polycentric systems of governance. It aims at convening scholars who are addressing cybersecurity policies from different angles, in order to trigger a discussion about if and how cybersecurity is emerging as a

specific domain of public policy.

We call for papers that present new theoretical and methodological reflections, as well as empirical research, on the institutionalization of cybersecurity and the related processes of policy-making. Submissions are particularly welcome on the following possible topics:

New frameworks and methods for the study of cybersecurity policies;
Typologies of cybersecurity policy;
Policy discourses on cybersecurity;
National and transnational policy networks;
Cybersecurity strategies and policy designs, and their implementation;
Implementation and adaptation of policy instruments in the cybersecurity arena;
Evaluation of cybersecurity policies;
Cybersecurity and foreign policy;
Epistemic communities and cybersecurity policy entrepreneurs;
Cybersecurity policy and politics;
Cybersecurity policies in public administrations;
Cybersecurity policies and emerging policy principles (e.g. digital sovereignty, digital constitutionalism);
Cybersecurity policies and emerging technologies (e.g. artificial intelligence, IoT, metaverse, quantum computing)
Cultures and ideologies of cybersecurity.

Accepted papers are expected to share new knowledge on cybersecurity policy, including analytical frameworks, comparative analyses and in-depth case studies. The panel will take place from the 27th to the 29th of June 2023 on-site in Toronto, though allowing remote presentations. The deadline for submission is the 31st of January 2023, and accepted papers will be notified by the 15th of February 2023.

P11 / Cybersecurity: policymaking and institutionalization

Chair : Mauro Santaniello (Università degli Studi di Salerno)

Second Chair : Jonathan Kamkhaji (European University Institute)

Third Chair : Giancarlo Vecchi (Politecnico di Milano)

Fourth Chair : Francesco Amoretti (Università degli Studi di Salerno)

Session 1

Tuesday, June 27th 15:50 to 17:50 (POD361)

The social dimensions of Cybersecurity governance: theoretical and empirical challenges

Maria Stella Righettini (University of Padova)

Cyber dangers and cybersecurity policy: an analysis of post-incident learning strategies

Francesco Maria Scanni (Universitá degli Studi di Teramo)

Simone Busetti (University of Teramo)

(Virtual) A local perspective on global challenges - Anticipating administrative digital security challenges

Willem Bantema

(Virtual) Gradually and then suddenly: the evolution of cyber security policy in Lithuania in response to focusing events

Ram?nas Vilpišauskas (Vilnius University)