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)

Since the Covid-19 pandemic, cybersecurity has emerged as a matter of extreme urgency in ensuring the European economy's and society's resilience. Cybersecurity policy covers all aspects of prevention, forecasting, tolerance, detection, mitigation, removal, analysis, and investigation of cyber incidents (ENISA 2017). In addition, the EU Cybersecurity Strategy adopted in 2013 fosters cyber resilience with a security-by-design approach based on adequacy, accountability, subsidiarity, and cooperation principles. The drivers of cybersecurity resilience are cybersecurity expertise supported by private operators, academia, research, and civil society awareness.

The increase in cyber-attacks and vulnerabilities has led to a renewed commitment to protecting infrastructure and society and raising cybersecurity awareness. However, several studies have shown a lack of understanding contributes to the growth of cyber-attacks (Khader et al. 2021).

Cybersecurity awareness is an area of recent focus (Wang et al. 2018). It can be described as public understanding of threats (ability to identify types of threats, judge their riskiness and be proactive, prevent or solve problems and demand solutions), knowledge of vulnerabilities (ability to adopt safe behaviors), (Ibidem), and the claim for education (from private citizens and current and potential professionals). In addition, it generates public value by establishing an inclusive, citizen-oriented, and data-driven discussion that raises awareness and contributes to policy and behavioral change (OECD 2021).

The paper argues that through public communication, cybersecurity authorities contribute to cybersecurity awareness and resilience. Based on the theory that distinguishes two ways of approaching public communication (public communication as power or as a service) (Macnamara 2017), the research investigates and compares digital media and social media cybersecurity policies in Italy and France to highlight different styles of boosting public awareness.

Using textual analysis, the paper investigates and compares the digital public communication on cybersecurity during 2022 by the leading Cyber security authorities of two EU Member States, Italy and France, and assesses citizens' engagement in public communication through a content and sentiment analysis of Twitter interactions (Vasconcellos-Silva et al. 2017).

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)

The extraordinary expansion of digitalisation has increased the vulnerability of public and private actors to cyber threats. Fraud, identity theft, terrorist attacks and cyber extortion are no longer sporadic phenomena but affect the daily lives of citizens and public institutions. The multiplication of cybersecurity problems and the increasing reliance on data and information systems by governments, public administrations, businesses and individuals raises several questions about the appropriate administrative, organisational and policy tools to deal with such events. The COVID -19 pandemic and the Russian-Ukrainian war have further accelerated this dynamic and increased the importance of the public policy of cybersecurity.

However, research on which instruments are most effective and under which political and institutional conditions they can work is still at an early stage. While the rise of cyber risks threatens our institutions, an

evaluation of policy responses—their design, formulation and implementation—is critical to assess and improve effectiveness.

This article presents a desk review of the evolution and policy instruments of the Italian cybersecurity policy. In addition, it offers a first analysis of the incident-response strategy of public administrations within the National Cybersecurity Perimeter. The selected case studies aim to investigate how incidents and cybersecurity crises trigger learning processes in the selected administrations and how such learning feeds into policy change.

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

Willem Bantema

This contribution focuses on administrative digital security challenges for the next 5-10 years so that municipalities can prepare. NHL Stenden University of Applied Sciences (Netherlands) conducted an exploratory study to increase insights and provide administrative tools to anticipate these digital developments. Theoretical insights and 7 interviews were used to make future scenarios. The scenarios are predominantly based on the insights that the researchers have gained from their research in the field of law enforcement and technology over the past five years and on knowledge of the literature on the municipal digital security domain. Interviews with experts were used to validate and supplement the scenarios. Some of the scenarios were tested with practitioners in public administration to identify central problems and action gaps.

The contribution will highlight the main conclusions whereby for the main municipal task areas in the field of digital security. This includes - directing role on cyber resilience, digital security of public events, prevention of public order problems caused online, and preventing and acting on a cyber crisis or cyber incidents. In developing the scenarios, account was taken of social developments that go hand in hand with digitisation: increasing social complexity and (despite this) an increase in organisational and information capacity among citizens and organisations.

From the fourteen scenarios (and input from expert meetings), five main lines emerge that municipalities can work with and where strategic choices must be made to be decisive in a digital society. In each task area, attention can be paid to these main lines. These are knowledge position (1), powers (2), monitoring (3), collaboration (4) and ethics (5). Ethics, and with it the question "What kind of a municipality do we want to be?", has a separate position and will have to be addressed in each main line for the development of policy on digital security and digitization. The core of complex exercise will be addressed, and discussion is welcomed. The strategic questions can help different companies make policies on digital security.

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

Ram?nas Vilpišauskas (Vilnius University)

The paper will analyse the impact of focusing events (in this case, cyber attacks and incidents in Lithuania and abroad) on the creation and evolution of cyber security policy in Lithuania. The main puzzle to be addressed and explained is the initial very slow establishment of cyber security as a new domain of public policy from 2007 to 2015 and later its fast reform and institutional consolidation in 2017-2018 leading to a remarkable improvement of Lithuania’s cyber security assessments in the Global cyber security rankings. The public debate on the need to have a cyber security policy was first triggered by cyber attacks against Estonia’s state institutions in 2007 and reinforced in 2008 when similar attacks were experienced by Lithuania’s institutions. The concrete policy proposals were drafted soon afterwards but it took 7 years until they have been approved by the Government and adopted by the Parliament. Even then they have been considered insufficient as the responsibilities for different elements of cyber security remained split between large number of institutions. New legal changes were prepared and adopted in 2017-2018 which resulted in institutional consolidation under the National Cyber Security Centre of the Ministry of Defence. Around the same time Lithuania has also become a visible actor in EU cyber security debates becoming the leading member state responsible for the EU rapid response cyber force.

Using the insights from the public policy literature on the impact of crises and other significant events on public policy and institutional change as well as frameworks such as punctuated equilibrium and advocacy coalitions the paper will present how accumulation of cyber security attack and incidents, especially the evidence of Russian cyber attacks against Ukraine in 2014-2016, led to the establishment of cyber security policy domain in Lithuania, and how this process was affected by domestic and external factors such as

political attention, leadership and learning from other countries (facilitated by the EU and NATO institutional settings). The paper will use a process tracing methodology relying on extensive media analysis (around 3700 news messages generated by the Baltic News Service after a search with keywords “cyber security”) and semi-structured interviews with the decision-makers and cyber security experts who played an active role in those policy decisions. The analysis has already been done as one of four case studies prepared within the project funded by the Lithuanian Research Council on resilience of welfare institutions in Lithuania and the impact of significant events in adapting to systemic risks in 2004-2020 (conducted in 2021-2022). The panel on cyber security at the IPPA conference thus provides a good opportunity to present the analysis in English language and contribute to theoretically sound and empirically informed debates on the creation and evolution of cyber security policies in democratic polities.