(Re)structuring power in the cyberspace

Policy and governance challenges to the production of state cybersecurity policies

Author

Mattia Sguazzini

PhD Candidate

Ph.D. Program in Security, Risk and Vulnerability, curriculum of Security & Strategic Studies, Università di Genova (Italy)

Preferred working group

Security and Defense Policy Strategy

Abstract

What policy space do states have in cyberspace? How do they design their cybersecurity policies? The literature on cyberspace governance emphasizes the limited role of states concerning their ability to frame policies independently and stably in clearly defined political arenas. The framework of conflicting or cooperative relationships between states and semi-state or non-state actors influences the range of opportunities and constraints for the agency of individual states with respect to cybersecurity policies. Such policies must also consider the different logics that drive the dynamics in different strategic environments as well as the possible interdependencies between them. On the other hand, states have room to define the scope and content of policies in cyberspace. The gap identified in the literature concerns the under-theorization of the domestic governance of cyberspace, particularly concerning the connection between constraints and opportunities in policy design dynamics.

This study aims to frame the policymaking of states given the domestic and international context of existing power relations and simultaneously consider the possibilities that the same states have of conditioning that context through their own policymaking.

Furthermore, this study aims to develop an object-centered conceptual framework, focusing on the analysis of the main components of cyberspace (divided into physical, transmission/logical, and application/content levels). This approach is useful for understanding which actors, at different governance levels, have the possibility of exercising power in relation to individual components. In this

way, it is possible to understand which actors act in the governance of different objects, and thus identify the (current and potential) policy space of the single states.

The first section provides a literature review aimed at framing the problem on which this study is based. In the second part, I explicate the research design and theoretical framework, developing an object-centered conceptual framework and a policy design typology capable of categorizing across domestic-foreign boundaries. In the third part, I present findings concerning the identification of the actors responsible for the governance of different cyberspace objects. In the fourth part, in light of the policy spaces identified in the previous section, I analyze what kind of policies EU states have put in place in the field of cybersecurity. In conclusion, I summarize and discuss the findings, outlining possible future research directions, with a focus on the possible applications of the study to assess the effectiveness of cybersecurity policies in relation to limiting the strategic outcomes of cyberoperations.

This paper is part of broader research that constitutes my PhD project. At the current stage of the study, I mainly consider employing qualitative methods (conceptual analysis and content analysis for the object-centered conceptual framework, and content analysis and interviews for the definition and identification of the states' policy spaces). At the moment, I am still testing the possibility of employing mixed methods, with two possible perspectives: the first concerns the triangulation of the qualitative findings with multivariate analysis to verify the different policies employed by the analysis units with respect to the different objects, and the second concerns the analysis of the positioning of states within international organizations using quantitative text analysis techniques (mainly LDA or seeded-LDA) to verify the possible coherence between domestic strategies and foreign policy.