Guest editorial

Milton Mueller and Farzaneh Badiei

Milton Mueller is Professor and Farzaneh Badiei is Research Associate at School of Public Policy, Georgia Institute of Technology, Atlanta, Georgia, USA.

Cybersecurity and internet governance: introduction to the special issue

Cybersecurity is one of the frontiers of *digital policy, regulation and governance.* The growing linkage between cyberattacks and state actors adds a national security and foreign policy dimension to the problem, complicating efforts at global cooperation. This special issue focuses on the way problems related to information and network security challenge existing institutions of governance. It is particularly concerned with the impact of cybersecurity policies on internet governance.

Two decades ago novel institutions, most notably Internet Corporation for Assigned Names and Numbers (ICANN), were formed to respond to the rise of a global internet. The new internet governance institutions departed from the traditional sovereignty model to empower non-state actors in a multistakeholder model of globalized governance. Some have argued that the link between cybersecurity and national security requires moving back to a more traditional sovereignty model on the internet. Yet the factors that led to transnational governance innovations like ICANN are also present in cybersecurity: global technical compatibility, globalized markets for technology and services, a need for cooperation and information sharing across jurisdictions and the need to avoid technical and economic fragmentation of online capabilities.

Will cybersecurity elicit institutional innovations, or will national security concerns lead to a renationalization of the internet? If the latter, what consequences will this have for global internet governance? Can internet governance offer lessons and models for institutional solutions to cybersecurity problems? The papers published here explore those questions. These papers come out of a workshop organized by the Internet Governance Project (IGP), which is part of the Georgia Tech School of Public Policy. The IGP workshop featured a complementary and interdisciplinary mix of academic researchers, industry representatives and military and public policy practitioners.

The opening paper by Milton Mueller, "Is cybersecurity eating internet governance?" attempts to conceptualize the relationship between internet governance and cybersecurity governance. It discusses and evaluates definitions of cyberspace, cybersecurity, national security, cybersecurity governance and internet governance in an attempt to develop an understanding of the degree to which internet governance and cybersecurity governance are interdependent, or competing and hostile models.

Unlike Mueller, Michel van Eeten sees little threat that cybersecurity will become the entering wedge for a renationalization of cyberspace. In his view, the "war" between nation state and transnational internet governance is only taking place at the level of discourse, which is at best loosely coupled to actual control over internet resources and policy. His paper, "Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity", surveys a range of case studies to study how the institutional landscape of security governance is "patched" to deal with emerging threats. While Michel van Eeten recognizes the emergence of state actors as major attackers in cyberspace, he sees no transformation of defensive cybersecurity; most governance of

DOI 10.1108/DPRG-07-2017-0036

cybersecurity is still in the hands of the owners of key internet facilities and resources, which are not states.

A unique historical perspective on the relationship between cybersecurity and internet governance is provided by Bradley Fidler's "Cybersecurity governance: a prehistory and its implications". Fidler's paper explains how in the early formative period of the Arpanet, in the 1970s, the US Department of Defense separated the research and management regimes for networks and network security, with the latter restricted to the military networks and network connections. This ordering of networks and security had enduring technological, political and even cultural consequences, which are breaking down today.

Brenden Kuerbis and Farzaneh Badiei engage in an ambitious effort to present a holistic overview of the way cybersecurity governance actually works. Their paper, "Mapping the cybersecurity institutional landscape", catalogues the role and interaction of three distinct governance structures in global cybersecurity: markets, hierarchies and networks. They make important observations about the differences between ex post and ex ante attempts to govern cybersecurity, and pave the way for future research on how institutional frameworks are related to improved security.

Finally, Jon Lindsay's paper "Restrained by design: the political economy of cybersecurity" makes an intriguing and original argument that cyberspace itself is a complex global institution with contracts embodied in both software code and human practice. Lindsay's work challenges many prevailing threat narratives and understandings of cyber conflict. In his view, "cyber conflict is a form of cheating within the rules rather than an anarchic struggle, more like an intelligence-counterintelligence contest than traditional war". Cyber conflict is, therefore, "restrained by the collective sociotechnical constitution of cyberspace, where actors must cooperate to compete".

Through historical, empirical and analytical perspectives, the authors of this special issue provide new insights for cybersecurity and clarify its linkage to internet governance, which can be useful for future policy and academic endeavors in this field.