Regulating cybersecurity: incentives, interventions and the emerging governance of the Internet

Abstract:

The Internet and its transboundary character pose challenges to existing regulatory frameworks and governance structures. While the state traditionally has been the predominant actor in international relations, especially when it comes to security issues, its role in the governance of the Internet seems limited. Moreover, the focus of the dominant theoretical perspectives on institutionalized international organizations burdens them with a critical blind spot as a large part of Internet governance appears to take place outside of such organizations.

In this talk, I will argue that the area of Internet security, primarily concerned with the threat of malicious software ('malware'), is not dominated by governments and not highly institutionalized. Instead, governance emerges from the daily interactions of thousands of private actors all over the world in rather informal networks. While originating in criminal behaviour and enabled by technical vulnerabilities, I will show that the magnitude and the impact of the malware threat is strongly influenced by the decisions of legitimate market players, such as Internet Service Providers, web hosting companies, software vendors, and e-commerce companies. Thus, a key challenge in regulating cybersecurity is strengthening the *incentives* of these so-called Internet intermediaries to invest in security. I will argue that the state still has a role to play, through *interventions* aimed at incentivizing private actors, but its role drastically changes, as for instance can be seen from new forms of collaboration with Internet intermediaries.

I will illustrate this argument empirically by the findings of recent multi-method research into how the markets for Internet services deal with security risks. In this research, we conducted in-depth interviews with professionals of organisations operating in networked computer environments that are confronted with malware. We also analysed large-scale incident data, often using computer science approaches and tools to connect this data to real-world organisations, markets and states. The aim is to develop metrics that express security performance across such organizations, markets and states and to detect factors (incentives, interventions) that affect such performance.

In the talk, I will consider what the implications of our findings are for current theoretical models of regulation and governance and how these models in our view have to be adjusted to be able to account for the *emerging governance* of Internet security.

Short Bio:

Martijn L.P. Groenleer (m.l.p.groenleer@tudelft.nl) is Associate Professor of Public Policy and Management at the Faculty of Technology, Policy and Management, Delft University of Technology, where he has worked since 2007, and a visiting professor at the London School of Economics and Political Science's Centre for Analysis of Risk and Regulation. He graduated in public administration from Leiden University in 2003, studied at the *Institut d'Etudes Politiques* (Sciences Po) in Paris, worked as a policy adviser (and member of the Task Force International Criminal Court) at the Netherlands Ministry of Foreign Affairs, and received his doctorate (*cum laude*) from Leiden University in 2009. In recent years, Martijn's research has focused on the analysis of regulation and governance in multilevel settings, notably the EU but also the US, and the study of (organizational) decision making in multi-actor networks. Currently, he is involved in research projects investigating, among others, the value of regulatory fragmentation and overlap in multilevel energy governance, the effectiveness of new forms of public-private collaboration in the fight against subversive, organised crime, and the role of market incentives and government interventions in the regulation of cybersecurity.