International Engagement on Cyber III

A great deal has transpired in the cyber realm during the past year. Concerns continue to mount over the security of customers’ financial and personal information after major retail chains, including Target and Neiman Marcus, experienced compromising intrusions. Debates regarding the distribution and regulation of cryptocurrencies continue unabated. The sophistication and impact of ideological hacking collectives, such as the Syrian Electronic Army and those affiliated with Izz ad-din al-Qassam, dramatically increased. Yet, no single story better reflects this past year’s cyber zeitgeist than the Edward Snowden revelations, which exposed the far-reaching surveillance and data collection apparatus crafted by the United States’ National Security Agency.

These events, particularly the Snowden Affair, have drastically shaped the debate over state power projection and its consequences. Global public discourse previously tended to center upon the Internet as a democratizing force, capable of weakening the control of the nation-state. The Internet transcended national borders and empowered the masses at the expense of traditional power blocks. However, this battle for the control of cyberspace is far from over. The nation-state is attempting to retrench its power in the digital realm, and the forces of centralization are appearing to gain strength in the struggle between diffusion and consolidation. This shift has raised serious questions regarding the responsibilities and limits of government cyber control.

State Building on a New Frontier — the third edition of our annual International Engagement on Cyber series — attempts to explore some of these difficult themes. The issue begins with a pair of pieces that discuss the nature and possibility of inter-state cyber conflict. Jan Neutze and J. Paul Nicholas identify norms that actors should cultivate to assuage growing ’cyber insecurity,’ while Roger Hurwitz proposes a number of state-driven policy shifts that might unilaterally decrease inter-state tension. Elaborating on this state-centric model of structuring cyberspace, Chris Demchak and Peter Dombrowski discuss the development of robust institutions of state sovereignty in the digital domain, while Ronald Deibert offers an alternative model to conceptualizing statecraft and interactions within civil society over the Internet.

Homing in on a particular aspect of nation building — establishing a credible defense infrastructure to protect domestic ‘territory’ from foreign incursion — Michael Warner and Michael Good propose an insightful new framework for state-based cyber deterrence efforts, while Catherine Lotrionte applies classic theories of international norm creation to this critical facet of national cybersecurity strategy. Lotrionte highlights how the United States has successfully driven this alternative track of development, which runs parallel to the failing interest-based efforts at deterrence. Samuel Visner rounds out this discussion of U.S. cyber policy by highlighting the tough decisions that nation-states must make to institutionalize their presence in cyberspace.
International Engagement on Cyber III: State Building on a New Frontier also features articles that deal with the technical side of the cyber discussion, namely attempts to create appropriate standards for continuing infrastructure development. Whereas discussion has previously focused on the manner in which the private sector drives innovation for sluggish state entities, Jeffrey Carr identifies data classification techniques related to new paradigms of cybersecurity that run contrary to this conventional wisdom. Francesca Musiani delves into the debate surrounding the current domain name system, while Andrea Rigoni applies knowledge management theory to information sharing strategies in the digital age. John Mills concludes the issue with an article that offers one perspective on how developments in cybersecurity relate to larger issues of force posturing in an increasingly multipolar global system.

We are very fortunate to have worked with such incredible experts in producing this issue, and want to thank our authors for their contributions to an excellent debate on the future of the state in this new digital frontier. We would also like to express our gratitude to Catherine Lotrionte, Director of the Institute for Law, Science, and Global Security, for her tireless support of this series. Please enjoy, discuss, and debate. We will see you next year with more cutting-edge policy and academic work in International Engagement on Cyber IV.