Cyberpolitik in the Post-Communist Era: The International Politics of the Internet, Cyberspace, and Cybersecurity

• David P. Fidler, James Louis Calamaras Professor of Law, Maurer School of Law; and Senior Fellow, Center on Applied Cybersecurity Research
• Padraic Kenney, Professor of History and International Studies; Director, Polish Studies Center; and Director, Russian and East European Institute
• Scott J. Shackelford, Assistant Professor of Business Law and Ethics, Kelley School of Business; and Senior Fellow, Center on Applied Cybersecurity Research

Provocation

The global emergence of the Internet as a communication technology, cyberspace as a political phenomenon, and cybersecurity as a policy concern largely occurred after the collapse of communism in the Soviet Union and Eastern Europe and China’s introduction of market reforms. As a result, the power, interests, behavior, and ideas of the United States—the dominant country of the initial years of the post-Cold War period—strongly affected the development of Internet governance, conceptualizations of cyberspace, and the framing of cybersecurity threats.

However, China, Russia, and countries once part of the Soviet bloc have, over time, challenged prevailing forms of Internet governance, tropes about cyberspace, and what constitutes a cybersecurity threat. Other countries, sometimes categorized as having authoritarian governments, have supported these challenges in diplomatic forums, and this support has helped the challenges gain traction and intensify political debates on these topics. More recently, the controversies the United States has experienced arising from Edward Snowden’s disclosures have put U.S. power, interests, policies, and ideas on the defensive at home and abroad in these policy contexts—a development China, Russia, and their supporters believe vindicates their positions.

The manner in which the international politics on the Internet, cyberspace, and cybersecurity have evolved in the post-communist era raise questions about what is happening now and what might unfold in the future. Analyzing these questions requires a deeper understanding of the domestic politics and foreign policies of post-communist and communist states on these issues. We pose the following questions about the role of these states in shaping contemporary cyberpolitik:

• What post-communist and communist states are managing to increase Internet access for their populations while simultaneously strengthening government capabilities to monitor, influence, and control their citizens’ behavior in cyberspace?
• How do Internet and cyberspace strategies in China, Russia, and like-minded post-communist states relate to obligations in international human rights law these states have to respect civil and political rights (e.g., freedoms of expression and association)?
• In other contexts, authoritarian governments have argued they prioritize economic, social, and cultural rights over civil and political rights to catalyze economic development. Does this perspective appear in the attitudes of China, Russia, and like-minded post-communist states towards Internet access and what citizens do with such access in cyberspace?
How do individuals, groups, and non-governmental organizations in post-communist and communist states perceive “cyberspace” politically, economically, socially, and culturally? Have these perceptions changed over time, and, if so, how have they changed?

Is it fair to characterize the positions of China, Russia, and like-minded post-communist states on Internet governance as “Internet sovereignty,” compared to the “Internet freedom” vision associated with the positions of United States and its allies? If not, how do these nations perceive political divides on Internet governance?

How are China, Russia, and like-minded post-communist states participating in multi-stakeholder processes that characterize Internet governance, including the ongoing effort to create new generic top-level domain names by the Internet Corporation for Assigned Names and Numbers (ICANN)? What problems do these countries have with these processes?

What value do China, Russia, and like-minded post-communist states see in the Internet Governance Forum (IGF), which is often criticized as little more than a “talking shop”? Do these countries support expanding the IGF’s mandate?

What impact has the Shanghai Cooperation Organization and its Agreement on Cooperation in the Field of International Information Security (2008) had on China, Russia, and like-minded post-communist states in dealing with cybersecurity threats?

How important to China, Russia, and like-minded post-communist states is the strategy of shifting diplomacy on Internet governance and cybersecurity more into the International Telecommunication Union (ITU), the UN specialized agency for telecommunication issues?

What did China, Russia, and like-minded post-communist states believe they achieved at the ITU’s World Conference on International Telecommunication in December 2012, at which ITU member states controversially adopted amendments to the International Telecommunication Regulations over the opposition of the United States and its allies?

How have the disclosures made by Edward Snowden been reported and discussed in China, Russia, and post-communist states? To what extent have these disclosures affected political discourse about the Internet, cyberspace, and cybersecurity in these countries?

How might Snowden’s disclosures affect the foreign policies of China, Russia, and like-minded post-communist states as diplomacy on Internet governance and cybersecurity continues in bilateral, regional, and multinational venues (e.g., finding common cause with other countries concerned about the disclosures, such as Brazil and Mexico)?

Why are China, Russia, and a number of post-communist states unwilling to become states parties to the Council of Europe’s Convention on Cybercrime, which is considered the leading international legal instrument facilitating cooperation on cyber crime as a significant global cybersecurity problem? What do these countries believe are realistic alternatives to the Convention on Cybercrime?

What are China, Russia, and like-minded post-communist states doing with their capabilities in cyber defense, cyber espionage, and offensive military cyber weapons? How do these states perceive existing international legal regimes that apply to cyber defense, cyber espionage, and the use of cyber weapons in armed conflict?

Looking forward, what do China, Russia, and like-minded post-communist states perceive will be the most important domestic and foreign policy issues involving Internet governance, cyberspace, and cybersecurity over the next decade?