Cybersecurity, International Law and Geopolitical Divisions

Professor Yarik Kryvoi

Last week cyberattacks against British Airways, BBC and Swiss government agencies made it to the top of headlines around the world. These attacks show that greater connectivity has increased vulnerabilities in the absence of global regulatory responses.

On 26 May 2023, we convened in Tokyo Symposium on 'Public and Private Governance of Cybersecurity: Challenges and Potential ' where we examined various aspects of cybersecurity regulation and why states cannot come up with truly global instruments to deal with cybersecurity. The event brought together academics, practitioners and policymakers from around the world to talk about regulatory responses to cybersecurity.

The participants noted that cyber governance is currently highly fragmented and involves not only states but other stakeholders, most importantly the private sector. States primarily regulate cybersecurity by adopting domestic legislation. However, the transborder nature of cybersecurity requires international cooperation, both at global and regional levels. The gaps in technical capacity and resources to deal with cybersecurity and deep divisions in understanding the purpose, that cybersecurity should serve makes such cooperation difficult.

Cybercriminals motivated by profit, ideology, or other reasons exploit greater connectivity to engage in attacks. The involvement of state actors (e.g., Russia or North Korea) makes tackling cyberattacks particularly difficult.

For some states (including the United Kingdom, the United States and Japan), the main purpose of cybersecurity is to protect networks, devices and data from unauthorised access and criminal use and human rights play a paramount role in this process. We label this model as market-oriented. In other states (including China, Russia, Saudi Arabia), the main focus of cybersecurity is on establishing state control and sovereignty over the Internet, often at the expense of human rights. We call this approach state-oriented.

In the book on public and private governance of cybersecurity, which we co-edited with Prof Tomoko Ishikawa from Nagoya we explain the geopolitical divisions between state-oriented and market-oriented models of cybergovernance. Cambridge University Press will publish this book in September.

By comparing domestic regulations and regional treaties, we highlight key distinctions between state-oriented and market-oriented approaches when it comes to the role of human rights, data protection, engagement of the private sector and the so-called content crimes. We argue that ideological and geopolitical differences as well as the gap in cybersecurity capacity prevent the creation of a truly global framework for cybersecurity regulation. However, such regulation is possible on limited matters, such as fighting child pornography.

Our chapter The Geopolitical Divide, Norm Conflict and Public-Private Partnership in Cybersecurity Governance co-authored with Tomoko Ishikawa explores in more detail the potential for regional cooperation and cooperation between like-minded states on cybersecurity as well as the role, which the private sector should play in this process.

The Tokyo cybersecurity symposium was organised by Nagoya University, the British Institute of International and Comparative Law and the Japan Forum on International Relations (JFIR), which hosted the event. It is a part of a multi-year project New Security Threats and the Future of Economic Globalization funded by the Japan Society for the Promotion of Science.

Author:
Prof Yarik Kryvoi, British Institute of International and Comparative Law

This blog post has also been published here.

URL: https://www.biicl.org/blog/63/cybersecurity-international-law-and-geopolitical-divisions