Global Policy Volume 7 . Issue 1 . February 2016

Governing Cyberspace: Building Confidence, Capacity and Consensus

Sash Jayawardane and Joris Larik
The Hague Institute for Global Justice
Mahima Kaul
The Observer Research Foundation

Special Section Article

Cyberspace is an integral part of modern societies and has transformed global social and economic relations in the 21st century. From an arcane and technical domain on the margins of international policy debates, cyberspace has entered the realm of high politics and is an important feature of contemporary debates on global governance. During the 2014 *India Conference on Cyber Security and Cyber Governance*, Indian academic and foreign policy analyst C. Raja Mohan opined that 'the age of innocence is over ... the widely held beliefs that cyberspace will be a libertarian utopia for individuals and a technological cornucopia for corporations now look utterly unrealistic ... the experiment in constructing a cyber world beyond states has come to an end'.[1] In other words, cyberspace is no longer the apolitical province of nonstate actors. Its power and ubiquity make it inherently political, and states increasingly seek to assert their sovereignty in this domain. While cyberspace presents unprecedented opportunities for economic growth, innovation and development, it also entails unparalleled risks. According to the chair of the 2015 *Global Conference on Cyberspace* (GCCS), 'the potential for malicious cyber activities by State and nonstate actors to create instability and mistrust in international relations is increasing'.[2] A clear need exists for building confidence, capacity and consensus among key stakeholders to ensure stability and predictability in international cyber relations.

Recognizing the growing importance of cyberspace in the foreign and security policies of states, as well as the economic prosperity and development of societies across the world, the 2015 GCCS called on all stakeholders to ensure that this global resource is managed in the public interest and remains 'free, open and secure'.[3] This special section provides insight into how freedom, openness and security can be achieved in cyberspace by making global cyber relations more stable, predictable and productive. It brings together four updated and revised contributions on cyber governance and cyber security that were first presented at the conference on *The Future of Cyber Governance* at The Hague Institute for Global Justice in May 2014.[4]

Chelsey Slack opens the special section by addressing how to improve international relations in the area of cyber governance in her article 'Wired yet disconnected: The governance of international cyber relations'. According to Slack, the networked structure of cyberspace – with its asymmetrical, anonymous and dual-use characteristics – as well as significant variations in the technological capabilities and political strategies of states, make it hard to establish consensus on international policy issues. She argues that while existing international legal regimes are adequate for effective cyber governance, further effort is required to link legal and political frameworks. Slack's analysis yields a set of policy recommendations to reduce uncertainty in international cyber relations and facilitate the development of norms for responsible state behaviour in cyberspace. These include: cultivating cyber security as both a national and foreign policy priority; calibrating the debate on cyber security in a manner that recognizes its military, political, economic and cultural dimensions, while focusing on areas where practical cooperation can build confidence among states; and bringing together likeminded states to build momentum around specific principles with the ultimate goal of forging international consensus ('minilateralism' in international cyber relations).

Mark Fliegauf analyzes the trust deficit in international cyber relations in his commentary entitled 'In cyber we trust', arguing that current efforts to govern interstate security issues in the digital domain are inadequate. According to Fliegauf, states are prone to exploiting the digital vulnerabilities of other states to access sensitive data and/or gain strategic advantages. He asserts that states generally favour private rent-seeking behaviour over producing a public good – global cyber security – which has led to the securitization, militarization and fragmentation of cyberspace. This results in a Catch 22 scenario: international governance structures are required to reduce the trust deficit that results from securitization and militarization, but the establishment of these structures requires a basic level of trust that is difficult to build under present conditions. Fliegauf writes that the US must take the lead in efforts to build the trust that must underpin any international governance architecture for cyber security. This can be done by improving on a recent track record of restraint under the Obama administration, which, for instance, declined to use cyber adjuncts to operations in Iraq and Libya over concerns about civilian casualties. Additionally, all states must resist the temptation to adopt cyber security strategies

that favour offence rather than defence, thereby mitigating the present security dilemma.

In 'Capacity building in cyberspace as an instrument of foreign policy', Patryk Pawlak explores cyber security capacity-building efforts undertaken by actors with advanced cyber capabilities, asking whether capacity-building can be a tool to further foreign policy goals. Several international players, including the EU, the US, China and Brazil, currently devote substantial resources to developing cyber strategies and capabilities at home and abroad that contribute to national security objectives and shape rules-of-the-road in this new governance domain. Based on two case studies – the Council of Europe's promotion of the Convention on Cybercrime (also known as the 'Budapest Convention') and the cybersecurity capacity-building efforts of the International Telecommunications Union – Pawlak finds that capacity-building in cyberspace is not a purely technocratic process, but rather one that is tailored to serve concrete foreign policy objectives. Pawlak concludes that while there is no single 'good' model for securing cyberspace through capacity-building, the exchange of best practices between countries and regional organizations may help streamline ongoing efforts. Importantly, capacity-building efforts should combine top-down and bottom-up processes, and reflect the actual needs of recipient countries as well as the shared values of donors and recipients.

Samir Saran concludes the special section with his commentary 'Striving for an international consensus on cyber security: Lessons from the 20th century', in which he reflects on global governance in previous centuries to discern lessons for how to govern cyberspace in the 21st century. Saran revisits major developments in global governance, including the codification of international norms on individual and collective rights, and multilateral treaty regimes in governance domains such as trade and climate. Turning to contemporary cyber governance, Saran argues that despite the interconnected, global nature of cyberspace, national laws, territoriality and sovereignty are more important than ever, with national governments retaining the primary responsibility for protecting basic rights. According to Saran, a comprehensive and robust global treaty on cyber governance is not feasible. Instead, efforts should be made to elaborate informal rules-of-the-road through strong bilateral cooperation and a vanguard of relevant stakeholders (a 'Digital 20'). These rules could translate into binding international commitments at a later stage. Saran notes that international treaties may be feasible for regulating specific, universally harmful aspects of cyberspace, such as the use of cyber weapons by nonstate actors. Constructive ambiguity in the language of formal treaties and informal codes of conduct can help forge consensus by avoiding the imposition of specific ideologies, and leaving governments sufficient leeway with regard to implementation. Saran concludes that the structure of cyber governance will thus be amorphous; an amalgamation of bilateral and multilateral treaties as well as informal codes of conduct.

The contributions presented in this special section seek to foster a better understanding of how to govern cyberspace – a domain that is complex, ubiquitous and an increasingly indispensable part of life in the 21st century. Despite the fact that cyberspace is primarily owned and operated by the private sector, the authors agree that states continue to exert a powerful influence over how cyberspace is used and governed. The contributions reveal that although cyberspace is a relatively new area of global governance, existing legal and political frameworks and traditional means and methods of conducting interstate relations remain relevant. A comprehensive, international treaty to govern cyberspace is unlikely to emerge in the near future. Therefore, a wide-ranging set of tailored efforts is required to ensure that cyberspace remains free, open and secure. Confidence and trust must be built between states and other relevant stakeholders through practical cooperation on specific issues, sharing information and best practices and exercising restraint in cyber activities. Bilateral cooperation and like-minded coalitions are essential for developing and disseminating norms or principles of responsible behaviour in cyberspace, which may set the stage for legally binding commitments in the future. Ultimately, the international architecture for governing cyberspace is likely to resemble the medium itself – an intricate web of actors, institutions and instruments securing a resource that is far greater than the sum of its parts.

Notes

1. Cited in: 'CYFY 2014: Outcome Statement', India Conference on Cyber Security and Cyber Governance [online]. Available from: http://cyfy.org/wp-content/uploads/2014/11/Cyfy-2014-Outcome-Statement-.pdf [Accessed 12 October 2015]
2. 'Chair's Statement', Global Conference on Cyberspace [online]. Available from: https://www.gccs2015.com/sites/default/les/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf, para 29. [Accessed 19 August 2015]
3. 'Chair's Statement', Global Conference on Cyberspace [online]. Available from: https://www.gccs2015.com/sites/default/files/documents/Chairs%20Statement%20GCCS2015%20-%2017%20April.pdf, para 5. [Accessed 19 August 2015]
4. The conference was organized by The Hague Institute for Global Justice and the Observer Research Foundation (New Delhi), with support from the Ministry of Foreign Affairs of the Netherlands. The aim of the conference was to allow cyber experts from different geographical and disciplinary backgrounds to engage in a rigorous analysis of contemporary challenges in cyber governance, in order to craft practicable policy recommendations to improve the governance of cyberspace. The discussions begun in The Hague continued in New Delhi at the India Conference on Cyber Security and Cyber Governance in October 2014. They also helped frame an official knowledge event at the Global Conference on Cyberspace in April 2015. These activities form part of the Global Governance Reform Initiative, a multi-year project that seeks to overcome challenges in key areas of global governance by improving the efficiency, effectiveness and legitimacy of collective actions undertaken by relevant stakeholders.

Author Information

Sash Jayawardane, Researcher on the Global Governance program at The Hague Institute for Global Justice. She served as Project Lead for the first phase of the Global Governance Reform Initiative project (2013–2015), which focused on the global governance of cyberspace.

Joris Larik, Senior Researcher on the Global Governance program at The Hague Institute and Assistant Professor of Comparative, European and International Law at Leiden University. His work has received several awards, including NATO's Manfred Wörner Essay Award (2008) and the EUI's Mauro Cappelletti Prize for the Best Doctoral Thesis in Comparative Law (2014).

Mahima Kaul heads the Cyber and Media Initiative at the Observer Research Foundation. Her recent publications include an essay on India's nod to multistakeholder Internet governance – 'The "I" in the Internet Must Also Stand for India' and an essay in the *ORF-Global Policy CyFy journal* – 'The Shifting Digital Pivot: Time for Smart Multilateralism'.