doi:10.1017/aju.2017.2

# INTRODUCTION TO SYMPOSIUM ON CYBERSECURITY AND THE CHANGING INTERNATIONAL LAW OF DATA

*Fleur Johns* and Annelise Riles*[†]

The hacking of the Democratic National Committee (DNC)'s email system and its resulting impact on the U.S. presidential election of 2016 has brought the issue of cybersecurity to the forefront of public concern in the United States and, to varying degrees, elsewhere. For the public, cybersecurity is no longer just a fringe problem of strange email scams promising unclaimed winnings, or a subject for off-beat television hacker dramas.[1] Now President Putin leaps to mind, as we are plunged into a newly perplexing version of Cold War intrigue. Even the most powerful of the world's nation-states seem to be at a loss as to how to respond. The Obama administration's struggles to craft a response to its finding that Russia hacked the DNC in an effort to influence the U.S. election, and the incoming Trump administration's dismissal of the episode as unworthy of further state action, have demonstrated the challenge that cybersecurity poses to international law, also. The existing toolkit of norms, treaties, institutions, and sanctions has been exposed as woefully inadequate.

As others have explained, cybersecurity is a term dating from the early 1990s that captures the imperative of countering a wide range of threats arising from the networked interpenetration of computer systems.[2] As such, it is by its nature a transnational problem with deep implications for interstate conflict and global economic order, as well as for individual and collective human rights. Yet as a discipline, international law is struggling to take account of technopolitical innovations that have a bearing on cybersecurity. First, cybersecurity stretches uneasily across existing international and national legal categories such as the laws of war, intellectual property law, criminal law, tort law, contract law, privacy law, the law and institutions governing the internet, and national security law. More importantly, the problems and possible solutions with which cybersecurity is concerned are not legal alone. They are also technical—framed by innovations in computer science hardware and software and in changing utilizations of these. And they are cultural too—determined by how technologies are deployed, and how norms are interpreted in diverse communities from hackers to email users, and from security professionals to product designers, around the world. Moreover the issues and problems look very different in different parts of the world. The cybersecurity problems and solutions in the most well-resourced countries are quite distinct from those of the developing world. As is often noted, the cybersecurity commitments of countries such as the United States or Australia and of the European Union stand in contrast to the more sovereignty-oriented frameworks advocated by countries such as Russia and China.

Any possible solutions will therefore depend on a rich international and interdisciplinary dialogue between lawyers, computer scientists, social scientists, economists, and humanists in different parts of the world. This is no

* *Professor of Law and Associate Dean of Research, UNSW Sydney.*

[†] *Jack G. Clarke Professor of Far East Legal Studies, Cornell University. The authors help to lead Meridian 180, a multilingual platform for policy solutions, which in recent years has sponsored a series of online international and interdisciplinary conversations on the subject of privacy, data, and cybersecurity, among other topics.*

[1] Noah Gamer, *Popular media depictions of hacker culture: Varying degrees of accuracy*, Trend Micro (July 16, 2015).

[2] Lene Hansen & Helen Nissenbaum, *Digital Disaster, Cyber Security, and the Copenhagen School*, 53 Int'l Stud. Q. 1155 (2009).

small challenge given existing barriers of language, disciplinary orientation, and sheer distance. The participants in this symposium hail from varied jurisdictions—the United States, Europe, Korea, Australia—and bring to the subject a wide diversity of expertise and epistemological orientations, including law, computer science, science and technology studies, anthropology, cultural studies, and hacker culture.

Taken as a whole, the symposium first highlights the limits of existing frameworks and diagnoses some of the reasons for those limits. Legal scholar David Fidler chronicles international legal developments and the U.S. position on those developments in cases of internet freedom, cyberespionage, and cybersecurity.[3] Fidler is ultimately quite pessimistic about the strength and utility of existing international legal norms, and about their vitality in the face of the antipathy of the incoming Trump administration.

Computer scientist Fred Schneider describes the practical, political, and economic reasons why available state of the art technologies to defend against cyberattacks have not been, and are unlikely to be fully deployed.[4] He raises the very interesting question of trade-offs between the state's interest in protecting citizens and corporations against cyberattacks and the state's interest in surveillance of the same citizens, as well as others for national security reasons.[5] We (Johns and Riles), professors of law and Far East legal studies respectively, describe the limits of two key modalities of thinking about cybersecurity, which we term the "bunker" and the "vaccine."[6]

In response, the symposium suggests several avenues for further research, policy consideration, and individual and community activism. Economist Sung-in Jun emphasizes the hybrid nature of the DNC hacking as both a matter of national security and a matter of personal privacy.[7] Jun suggests using tools from the law of property and privacy law to distinguish cases and guide moral judgment about proper responses. Yet he points out that there is a trade-off, again, between individuals' interest in privacy and corporations' interest in access to individual information and also governments' interest in surveillance. Niranjan Sivakumar, a lawyer, hacker, and science and technology studies scholar, looks to science and technology studies and hacker culture for a more participatory approach to cybersecurity.[8] He gives examples of collaboratively developed technological solutions that demonstrate the value of "nonhegemonic configurations of knowledge and power as a source of novel and creative contributions" to the problem.[9] Two of the contributions—ours and Sivakumar—propose conflict of laws or private international law frameworks as useful supplements to public international legal approaches. In Sivakumar's case, this is because the conflict of laws enables a more participatory process of norm development. In our account, private international law techniques suggest a way of thinking about cybersecurity that is more attuned to the entanglements that cyberthreats exploit, and the overlapping jurisdictions that may bear upon them.

Sivakumar ultimately suggests that hacker culture can serve as a model, or an analogue, for how policymakers and international lawyers might fashion new solutions to cybersecurity problems. The challenges of doing this—of learning laterally, across different genres of expertise, and of working effectively across existing linguistic, cultural, and geopolitical hierarchies and divides—are daunting. But in another sense this has always been the core mission of international law.

[3] David P. Fidler, *The U.S. Election Hacks, Cybersecurity, and International Law*, 110 AJIL Unbound 337 (2017).

[4] Fred B. Schneider, *A Computer Scientist Musing about the DNC Hack*, 110 AJIL Unbound 343 (2017).

[5] See also the contributions by Sung-in Jun and Niranjan Sivakumar on this point.

[6] Fleur Johns & Annelise Riles, *Beyond Bunker and Vaccine: The DNC Hack as a Conflict of Laws Issue*, 110 AJIL Unbound 347 (2017).

[7] Sung-In Jun, *National Security or Privacy: A Second Thought on the DNC Hack*, 110 AJIL Unbound 352 (2017).

[8] Niranjan Sivakumar, *Generative Security: Adversarial Design and Conflicts of Laws*, 110 AJIL Unbound 358 (2017).

[9] *Id.* at 358.

https://doi.org/10.1017/aju.2017.2 Published online by Cambridge University Press