doi:10.1017/aju.2019.30

INTRODUCTION TO THE SYMPOSIUM ON CYBER ATTRIBUTION

*Monica Hakimi**

This symposium explores some of the legal issues surrounding the attribution of cyber conduct to states. Relative to states' other activities, cyber conduct poses particularly thorny attribution challenges. States that engage in such conduct often use technology to obscure their identities or the full effects of their operations. The attribution challenges in turn raise difficult questions about how victim states should be allowed to respond—whether in kind, with other retorsions or countermeasures, with kinetic force, or by doing nothing at all. For example, how confident must a victim state be that it has correctly identified the source of the attack before responding? Should its degree of certainty depend on whether it believes that the cyberattack amounts to an "armed attack" under the *jus ad bellum* and thus triggers the right to use defensive force? And how much information, if any, must the victim state disclose about the attack or its author in order to justify a response?

The first essay in the symposium, by William Banks of Syracuse University, sets the scene for what follows.[1] It discusses the nature of the attribution problem in the cyber context, as well as some impediments to and opportunities for international legal regulation. Banks ultimately suggests that states have not established an effective framework for regulating cyberattacks. In his view, the current framework is only rudimentary and is unlikely to curtail harmful cyber conduct.

Berenice Boutin of the Asser Institute then examines the possibility of holding multiple states responsible for a single cyberattack.[2] Boutin argues that, given the difficulties of attributing such conduct to states, shared responsibility might be a useful way to "broaden the net of possible responsible states in relation to a cyber operation." Boutin considers three scenarios in which shared responsibility might be appropriate: (1) when states jointly conduct a cyberattack, (2) when one state aids or assists another in committing an attack, and (3) when a state fails to take reasonable measures to prevent its territory from being used for attacks.

Lorraine Finlay and Christian Payne of Murdoch University in Australia consider the attribution of cyberattacks that might qualify as armed attacks under the *jus ad bellum*.[3] Finlay and Payne explain that the challenges in identifying the source of a cyberattack have two significant implications for the *jus ad bellum*. First, they increase the risk of misattribution and thus of conflict escalation, if a victim state mistakenly retaliates against an innocent third party. Second, because a victim state will generally need time to identify the source of an attack, it might have difficulty satisfying the requirements of immediacy and necessity for lawfully using defensive force. After examining these challenges, Finlay and Payne argue that, although a victim state should satisfy a strict attribution standard if it wants to respond with force, it might reasonably apply a looser standard to respond with less severe measures. The result would be a variable attribution scheme, in which the appropriate standard for attribution depends on the nature of the victim state's response.

* *Professor of Law, University of Michigan Law School.*

[1] William C. Banks, *The Bumpy Road to a Meaningful International Law of Cyber Attribution*, 113 AJIL Unbound 191 (2019).

[2] Berenice Boutin, *Shared Responsibility for Cyber Operations*, 113 AJIL Unbound 197 (2019).

[3] Lorraine Finlay & Christian Payne, *The Attribution Problem and Cyber Armed Attacks*, 113 AJIL Unbound 202 (2019).

Chimène Keitner of the University of California, Hastings focuses on a particular response by the U.S. government—what she calls "attribution by indictment."[4] The phrase refers to the U.S. practice of using domestic criminal law to implicate foreign states in harmful cyber conduct. Keitner explains that this practice can serve at least three functions. First, it can incapacitate particular wrongdoers by publicizing their conduct and, if possible, apprehending them. Second, it can deter malicious cyber conduct by increasing the risks of engaging in that conduct. Third, it can serve an expressive function by helping to define acceptable standards of conduct, shame wrongdoers, or alert different audiences to U.S. detection capabilities.

Finally, UCLA's Kristen Eichensehr examines the efforts of nonstate actors to attribute cyber conduct to states.[5] For example, in a prominent early case, the cybersecurity firm Mandiant published a detailed report that attributed to a particular unit of the Chinese military hacking activities against over one hundred companies. Eichensehr explains that attributions by nonstate entities are often faster and more detailed than governmental attributions, and can fill important informational gaps. She concludes that, in today's political climate, there are real virtues to allowing multiple actors—some private, others public—to participate in attribution decisions.

On the whole, the essays in the symposium both highlight the challenges to attributing cyber conduct to states and offer some prospects for overcoming these challenges. The essays suggest that questions about the attribution of cyber conduct are quite difficult and are likely to be with us for some time.

[4] Chimène I. Keitner, *Attribution by Indictment*, 113 AJIL Unbound 207 (2019).

[5] Kristen E. Eichensehr, *Decentralized Cyberattack Attribution*, 113 AJIL Unbound 213 (2019).

https://doi.org/10.1017/aju.2019.30 Published online by Cambridge University Press