

INTRODUCTION TO SPECIAL ISSUE – SECURITY AND THE CENTRALITY OF JURISDICTION

Erin Gibbs Van Brunschot, University of Calgary

The concept of jurisdiction is foundational to understanding security and security threats. Jurisdiction is often equated with legal governance: an arena in which courts establish claims regarding whose laws apply, how, where, and when laws apply (Van der Woude, 2020). Yet beyond legal frameworks, our understandings of security are underscored by jurisdiction both real and perceived: from recognizing and naming threats, to addressing and managing threats, jurisdiction is the basis upon which choices regarding threats are made and if and what action is taken.

Traditional views of security consider the sovereign state the object of security; therefore, realist approaches maintain that state apparatuses, including the police and military, are best suited to ensuring (state) security in the face of threats (Deibert, 2018). Yet as the security landscape becomes increasingly complex, a polycentric view of security's objects and responses may better address contemporary threats. Deibert (2018) advocates a "human-centric approach" (p. 419) to security, one that may be more in keeping with the nature of today's threats – many of which ignore sovereign boundaries – including threats to water, food and energy, economic crises, and cyber threats, to name a few. A human-centric security approach aims at providing "resources to independent agencies at multiple levels of governance" (Deibert, 2018, p. 419).

Governance, pluralization, and resources provide a baseline to begin to understand the significance of jurisdiction to 21st century security. Drawing on the insights of geography, Valverde (2009), for example, explains the importance of 'scale' to understanding governance as it applies to security threats. Imagine, for a moment, Google Earth, which enables us to consider different scales or perspectives at various geographic locations – as scales change, so too does the governance and authority available to identify, manage, and address security threats. Security threats are dissimilar at different scales – what appears as a significant threat at one scale or level, may disappear or become even more threatening at yet another scale. Recognizing differences in scale underscores the complexity of governance and the differing meanings and responses to security threats.

How do **multiple levels of governance** apply to security threats? In the case of illegal migration, for example, Muniz (2019) considers domestic immigration surveillance and how it extends beyond physical borders. In the U.S., law

enforcement officials' use of "surveillance and control technology stretch outward to intercept immigrants before they reach the physical border territory and push inward to police migrants deep in the country's interior" (p. 1639). The 'push outward' means that the governance structures of immigrants' originating countries are involved in U.S. border operations at the same time local (municipal) police are implicated in surveillance activities associated with border (national) control. The nature of the security threat may require not only subnational cooperation but may also require international collaboration to address identified threats; security threats can be both local and global and subject to several levels of governance. Similarly, international efforts to address threats may also be impacted by 'glocalization', whereby local conditions temper global pressures (Baskerville & Grossi, 2019). Efforts at local levels may seek to "retain jurisdictional identity in the face of continental... or global pressures" (Baskerville & Grossi, 2019, p. 96). Threats may therefore appear different depending on who intends to govern; at the same time, accepting or forfeiting governance of security threats may occur at the local, national, or international levels.

While the realist conceptualization of security threats points to the state as the legitimate source of protection against threats, the state as object of security may no longer resonate in the face of today's threats. Bures (2017) notes that there is widespread agreement that "a **pluralization of security** is taking place... in several areas of (inter-)national security, private rather than public entities nowadays shoulder the bulk of the burden in responding to the new security threats, such as terrorism and organized crime" (p. 290). The jurisdictional relationship between public entities, such as the police and military, with private security organizations is not always straightforward. As Shearing and Stenning (1983) pointed out some time ago, while private security was once described as 'subcontracting' to public police agencies, over time, the provision of security has increasingly 'outgrown' what public police can offer with many organizations now providing their own security services. Cybersecurity is a typical example: public police have difficulties keeping up with quickly evolving technological changes and many organizations assume responsibility to address cyber threats themselves. Yet Meerts and Dorn (2009) underscore that the interests of those in the business of private security may run counter to what is perceived as the role of the state in the provision of security. As Bures and Carrapico (2017) note, security has become "increasingly transformed from a political problem requiring welfare social policy and state intervention to a technical problem amenable to private solutions through the logics of cost efficiency" (p. 237) and commodification.

Finally, Deibert's emphasis on **resources** as underpinning jurisdiction is central to the ways in which security threats are defined and managed. In Bierens, Boersma, and van den Homberg's (2020) examination of disaster preparedness, for example, they underscore the importance of "impact-based forecasting" (p. 446); resources are pivotal when considering the magnitude of the security threat and the resulting impact. Vulnerability is highly contingent on the resources enlisted to identify and anticipate security threats, as well as the ability to deal with disaster and security threats in the aftermath. If there are few resources to address certain threats, these may be considered less threatening and therefore outside of an organization's purview or responsibility. Similarly, in their research on energy supply chains, Healy, Stephens, and Malin (2019) refer to the transboundary impacts of energy decisions and the "unequal distribution of costs, risks and vulnerabilities" (p. 220). In the pursuit of energy security at the receiving end of a supply chain, the costs for those in other parts of the supply chain can be significant. The importance of resources for jurisdiction is also emphasized in the adoption of climate action plans. In their study of climate action policy, Hui, Smith, and Kimmel (2019) found a positive correlation between "local climate policy adoption and population size, education level, and income level" (p. 493). In other words, those who have more resources with which to address security threats (such as climate change) will be more likely to adopt policies designed to address such threats.

Although "jurisdictions' ancient partnership with sovereignty tends to privilege territory" (Valverde, 2009, p. 154) – Valverde also reminds us that there are limits to conceiving of jurisdiction as being only about territory. Why or how various threats become security issues is also related to temporality. Governance structures evolve over time, as do the actors involved in the provision of security and the resources that actors have at their disposal. Cyber security and climate change, for example, have only in recent decades appeared on the 'security threat radar'. Understanding how security threats come to be identified, managed, and addressed requires a deeper understanding of the historical contexts in which threats are situated.

Finally, how we consider the elements of jurisdiction - **governance**, **pluralization**, and **resources** – has implications for our understandings of accountability and responsibility, oversight and transparency, and legitimacy. Those who claim jurisdiction over security threats become accountable and responsible for addressing such threats. At times, however, as researchers have observed, not all entities who claim jurisdiction have been open to external oversight and transparency. As Woods (2017), for example, notes, "the United

States military justice system enjoys unique autonomy from the purview of civilian oversight” (p. 1349). As more agencies enter the arena of security provision, competition might increase the likelihood of external oversight. Transparency may also be facilitated by a competitive market for delivering security and bolster consumer choice. While a shift to pluralization of security may open up the floodgates to a number and range of security providers, each of which might claim jurisdiction over a security threat, these entities must not only address the security threats they promise to be responsible for but must also secure their legitimacy as the appropriate provider of the security they claim to offer.

References

- Baskerville, R., & Giuseppe, G. (2019). Glocalization of accounting standards: Observations on neo-institutionalism of IPSAS. *Public Money & Management, 39*(2), 95–103.
<https://doi.org/10.1080/09540962.2019.1580894>
- Bierens, S., Kees, B., & van den Homberg, M. J.C. (2020). The legitimacy, accountability, and ownership of an impact-based forecasting model in disaster governance. *Politics and Governance, 8*(4): 445–455.
<https://doi.org/10.17645/pag.v8i4.3161>
- Bures, O. (2017). Contributions of private businesses to the provision of security in the EU: Beyond public-private partnerships. *Crime, Law and Social Change, 67*(3), 289–312.
<https://doi.org/10.1007/s10611-016-9650-6>
- Bures, O., & Carrapico, H. (2017). Private security beyond private military and security companies: Exploring diversity within private-public collaborations and its consequences for security governance. *Law and Social Change, 67*(3), 229–243.
<https://doi.org/10.1007/s10611-016-9651-5>
- Deibert, R. J. (2018). Toward a human-centric approach to cybersecurity. *Ethics & International Affairs, 32*(4), 411–424.
<https://doi.org/10.1017/S0892679418000618>
- Healy, N., Stephens, J. C., & Malin, S. A. (2019). Embodied energy injustices: Unveiling and politicizing the transboundary harms of fossil fuel extractivism and fossil fuel supply chains. *Energy Research & Social Science, 48*, 219–234. <https://doi.org/10.1016/j.erss.2018.09.016>
- Hui, I., Smith, G., & Kimmel, C. (2019). Think globally, act locally: Adoption of climate action plans in California. *Climatic Change, 155*, 489–509.
<https://doi.org/10.1007/s10584-019-02505-7>
- Meerts, C., & Dorn, N. (2009). Corporate security and private justice: Danger signs. *European Journal of Crime, Criminal Law and Criminal Justice, 17*(2), 97–112. <https://doi.org/10.1163/157181709X429114>

- Muniz, A. (2019). Bordering circuitry: Crossjurisdictional immigration surveillance. *UCLA Law Review*, 66(6), 1636–1681.
<https://www.uclalawreview.org/bordering-circuitry-crossjurisdictional-immigration-surveillance/>
- Shearing, C. D., & Stenning, P. C. (1983). Private security: Implications for social control. *Social Problems*, 30(5), 493–506.
<https://doi.org/10.2307/800267>
- Valverde, M. (2009). Jurisdiction and scale: Legal ‘technicalities’ as resources for theory. *Social and Legal Studies*, 18(2), 139–157.
<https://doi.org/10.1177/0964663909103622>
- Van der Woude, M. (2020). A patchwork of intr-Schengen policing: Border games over national identity and national sovereignty. *Theoretical Criminology*, 24(1), 110–131.
<https://doi.org/10.1177/1362480619871615>
- Woods, A. (2019). A “more searching judicial inquiry”: The justiciability of intra-military sexual assault claims. *Boston College Law Review*, 55, 1329–1366. <https://lawdigitalcommons.bc.edu/bclr/vol55/iss4/9/>



This work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

© (ERIN GIBBS VAN BRUNSCHOT, 2021)

Published by the Journal of Intelligence, Conflict, and Warfare and Simon Fraser University

Available from: <https://jicw.org/>