

The Politics of Cybersecurity and the Global Internet

Jessica L. Beyer , University of Washington
jlbeyer@uw.edu

Semi-State Actors in Cybersecurity. By Florian J. Egloff. New York: Oxford University Press, 2022. 294p. \$99.00 cloth, \$29.95 paper.

Four Internets: Data, Geopolitics, and the Governance of Cyberspace. By Kieron O'Hara and Wendy Hall. New York: Oxford University Press, 2021. 360p. \$35.00 cloth.

The Politics of Cybersecurity in the Middle East. By James Shires. New York: Oxford University Press, 2022. 312p. \$49.95 cloth.

Many of the conversations about international cybersecurity have remained siloed in specific disciplines and professional cultures. As such, there is disagreement among academics and practitioners about how to define basic terms, such as “cybersecurity,” and arguments about what should “count” as part of cybersecurity. Because people’s perspectives on cybersecurity are often defined by where they “sit” professionally, practitioners and scholars are sometimes unaware that they do not share a conceptual universe. For instance, many separate international internet governance debates from conversations around global cybersecurity norms, although many of the same cleavages and barriers to agreements occur in both domains. Others consider censorship to be unrelated to cybersecurity, although espionage via hacking uses many of the same tools as the domestic surveillance that goes hand in hand with censorship. Still others do or do not incorporate considerations of internet infrastructure into conversations about conflict in spite of concerns about the security of undersea cables to most global powers. The three books under review—James Shires’s *The Politics of Cybersecurity in the Middle East*, Florian Egloff’s *Semi-State Actors in Cybersecurity*, and Kieron O’Hara and Wendy Hall’s *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*—all help us understand how to think about this landscape. Each untangles some of these disconnects by making assumptions transparent, articulating places of overlap, unpacking terminology and categories, and offering paths forward for scholars.

Of the three books, James Shires’s *The Politics of Cybersecurity in the Middle East* most effectively bridges disciplinary and professional siloes. Shires’s book creates a holistic look at cybersecurity politics that is grounded in a deep area understanding of the Middle East. This is perhaps unsurprising considering that he uses a combination of field work in numerous Gulf states where he spent time engaging in interviews and ethnographic work. He additionally unpacks the politics of cybersecurity with secondary sources such as leaked documents, official and semiofficial documents, multimedia artifacts, technical reports from private-sector actors, and investigative media reports.

Shires begins his book with three short stories from 2012: an account of the infamous Shamoon attack on Saudi Aramco, a UAE cybersecurity law that criminalized “content crimes” online, and the Citizen Lab’s discovery of the FinFisher digital surveillance tool on activists’ computational devices. Shires points out that all three of these occurrences are considered “cybersecurity” by some security experts but not by others. Cognizant of these divisions, instead of defining the concept “cybersecurity” itself, Shires centers his book on the politics of cybersecurity. He asserts, convincingly, that looking at how cybersecurity plays out in the Middle East as a region and moving the focus from specific definitions, actors, technologies, or activities allows for a grounded definition of cybersecurity to emerge. Shires’s focus on politics means that he is able to identify how different actors articulate cybersecurity in relation to their own interests. To conceptualize cybersecurity, Shires employs the concept of “moral

maneuvers,” defining them as “the alteration of value-based and technological claims within an expert field ... for strategic gain” (p. 4). He argues that actors engage in moral maneuvers under two conditions: (1) when a field, such as cybersecurity, becomes particularly lucrative, thereby attracting attention and resources; and (2) when understanding that field requires a high level of expertise (pp. 4–5). Shires argues that cybersecurity’s novelty means that it reinforces both its lucrativeness and reliance on expertise.

Shires asserts that Middle East politics scholarship and international relations (IR) theories have not engaged with each other substantively in considering cybersecurity issues, even when incidents that occur in the Middle East are featured in studies of cybersecurity or vice versa. Shires places his work at the intersection between the two, arguing that although many scholars and others conceive of the “internet” as a global issue, its form is deeply shaped by state politics, commerce, and laws. He argues convincingly for understanding the Middle East as an important area to explore the questions of cybersecurity politics, tying this work to both existing scholarship on cybersecurity and international politics as well as IR theories related to norms.

Shires divides cybersecurity into four categories: cyber conflict, human rights/targeted surveillance, foreign interference, and information controls. He uses these categories to structure much of his book. In relation to conflict, Shires focuses on Iran, which first appears in stories of international cybersecurity as the victim of one of the world’s most famous cyberattacks: the US and Israel’s 2010 Stuxnet attack. He uses this discussion to consider the overall development of cyberspace as an area of focus, unpacking the turn to “netwar” in post-Soviet Russia and the US in the 1990s. He points out that while many countries have developed offensive cyber programs, it is Russia, China, Iran, and North Korea that dominate public discussion.

Shires then turns his attention to the question of human rights and targeted surveillance as an arena of cybersecurity. A subset of cybersecurity experts would disagree that cybersecurity includes what could be considered a set of human rights concerns—the surveillance, censorship, targeting, and digital security of activists. They would argue that such issues are not about the security of networks and computational systems. However, Shires begins this chapter with a story about a presenter at a cybersecurity conference who called Egyptian protester Wael Ghoneim a cybersecurity threat, illustrating that for some in the field cybersecurity and human rights overlap (p. 111). As Shires points out, many nondemocracies include concerns about social stability or threats to the state in cybersecurity laws. Tied to this, he engages in a deeper discussion of how NGOs have used the symbolic and financial capital of cybersecurity as a concept to further human rights

objectives, at the same time that producers and exporters of surveillance technologies have used the term “cybersecurity” to frame the sale of their products.

While Shires divides targeted surveillance and information controls into two separate categories, they overlap in the sense that both focus on the idea that information and the use of information technology is threatening to states. In his discussion of information controls, Shires examines how cybercrime laws are employed to create information controls criminalizing some kinds of online content and opening markets to companies selling information-controlling technology. Shires points out that characterizing information controls as a cybersecurity issue gives it normative weight and normalizes state surveillance and controls.

Shires argues that “the conception of a national information environment itself is symbiotic with the identification of internal threats to that environment” (p. 202). He continues this argument by addressing the question of how actors strategically engage with the idea of “foreign interference,” focusing on how issues such as leaking, disinformation, and media ownership end up being defined as cybersecurity issues. Shires notes that these issues have long been studied and have been considered to overlap with cybersecurity; however, he illustrates that framing these issues as “cybersecurity” creates opportunities for some actors. As he does elsewhere in the book, he suggests that this expansion of cybersecurity is malleable and open for interpretation as actors operate to expand their political or economic influence.

Shires manages to incorporate many of the strands of the diverse discipline of cybersecurity into his book. However, in his attempt to incorporate everything, sometimes it is difficult to keep the strands separate. This is particularly the case in parsing his division between information controls and targeted surveillance—both having to do with censorship and human rights. That said, I have recommended Shires’s book repeatedly to people across disciplines who study cybersecurity, to people wanting an introduction to cybersecurity, and to students who want to learn more about how to think about cybersecurity politics in particular regions.

Shires’s book offers an effective bridge between disciplines and professional understandings of cybersecurity. In contrast, Egloff’s *Semi-State Actors in Cybersecurity* offers political scientists, in particular, important tools for understanding a pressing international issue that has lacked sufficient analytical engagement—the interaction and behaviors of nonstate, semi-state, and state actors in international cybersecurity. To do this, Egloff effectively uses sixteenth- to nineteenth-century piracy as a tool to analyze contemporary international cybersecurity politics.

Egloff argues that, analogous to the way earlier states treated pirates, privateers, and mercantile companies, present-day states rely on private cybersecurity actors to

act in state interests. Egloff asserts that, much like the present security dynamics of cyberspace, historical states worked to extend power into the ungoverned space of the high seas through work with or tolerance of nonstate actors. Therefore, the comparison of cyberspace and the sea is a fruitful arena for understanding relationships between actors. Egloff takes a middle path between arguments that cyberspace is an arena of state competition like any other in which states are the dominant and most important actors, versus arguments that cyberspace is a new phenomenon and a fundamental break from the past that challenges state power. Instead, he argues that cybersecurity competition between states is closely related to state “collaboration and competition” with semi-state actors.

Tying the history of the pirates, privateers, and mercantile companies of the sixteenth to nineteenth centuries to contemporary international cybersecurity, Egloff frames actors’ proximity to states as a continuum. In order to understand actor agency, the long-term impacts of privateering on security policy, and states’ concerns over private-actor behavior, he engages in archival research to create historical analogies and then draws on secondary sources to understand contemporary cybersecurity. Egloff articulates these cases and this approach in a series of illuminating tables in his methodology chapter, and then draws them out in the subsequent chapters in deep detail.

In his comparison of contemporary cybersecurity and the high seas, Egloff posits that state and nonstate actors cannot be divided easily into two separate categories. Instead, he creates three categories to capture greater gradation between actors, connecting sixteenth- to nineteenth-century categories to the present day. For example, he links state actors—intelligence, defense, police forces, and others who clock in nine-to-five jobs on behalf of governments—with the navies in that earlier period. He likens current semi-state actors, such as technology companies, patriotic hackers, private contractors, and some cybercriminals, to the mercantile companies and privateers of the past. Finally, Egloff connects today’s nonstate actors, specifically independent hackers and cybercriminals, to the pirates of the sixteenth to nineteenth centuries.

Egloff asserts that these historic relationships can serve as a means to understand how the attribution of attacks are a political tool that uses proximity to states not only to assign blame, but to shape actor categories. He follows this argument with one that focuses on the collaboration between cybercriminals and states, using the Russian state’s relationship to organized crime as the central example. Finally, he explicitly labels major technology companies such as Google and Huawei as political actors, using the mercantile companies of the past to again focus attention on the relationships between states and these companies. He points out that mercantile companies

strategically employed their proximity to states as they engaged in expansionary behavior.

In order to use piracy in the sixteenth to nineteenth centuries to understand contemporary cyberspace, Egloff must articulate the similarities and differences between the two domains. He captures similarities between the two, such as the role of geography, the costs of offensive and defensive capabilities, public–private divides in capabilities, the difficulty of attribution, and the dependence of actors on the domain. The differences he articulates are actors’ exposure to physical sanctions, the pace of technological change and diffusion of knowledge, international society and institutions, and the stability of domain characteristics. Having made the case for sufficient similarities, Egloff goes on to apply his framework to several well-known cybersecurity events: Russia’s alleged 2007 cyberattacks on Estonia (pirates and privateers); China’s 2009 Operation Aurora, with a focus on Google’s breach; and the North Korean 2014 Sony attack (cyber-mercantile companies).

The strength of Egloff’s book is the framework he offers to think about nonstate actors in international cybersecurity—one that does not treat hackers as having no historical antecedents. Of course, his case hinges on the reader’s acceptance of the appropriateness of the sixteenth to nineteenth centuries as a useful analogy for understanding present-day cyberspace. Some might question elements of this. For instance, he argues that key strategic sea lanes are similar to global internet infrastructure, ignoring that internet infrastructure is not finite or fixed in the way that a sea lane might be. Nevertheless, these are small quibbles and his use of the past grants analytical leverage and offers a model for other researchers. I have recommended his book to many others since reading it.

Egloff misses an opportunity to connect his work to other disciplines because he does not directly engage with the literature on digital pirates as political actors. There is a long history of hackers, hacktivists, and cybercriminals employing the concept of piracy as tied to a political philosophy that incorporates evasion of state authority as a central driving element (see Jessica Beyer and Fenwick McKelvey, “You Are Not Welcome Among Us: Pirates and the State,” *International Journal of Communication*, 9, 2015; Chris Land, “Flying the Black Flag: Revolt, Revolution and the Social Organization of Piracy in the ‘Golden Age,’” *Management and Organizational History*, 2(2), 2007). Not only that, but piracy is closely linked to hacking culture, and the concept of hacking has served as a catchall term for many political projects that are grounded in state resistance (refer to Patrick Burkart, *Pirate Politics: The New Information Policy Contests*, 2014; Gabriella Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking*, 2012; and Christopher M. Kelty, *Two Bits: The Cultural Significance of Free Software*, 2008). The imagery of pirates has been a powerful political tool both in realms

where piracy is explicitly employed—such as file-sharing sites (Beyer and McKelvey 2015)—as well as more broadly in hacker communities working to create state-evading tools, such as secure and anonymous communication (Andy Greenberg, *This Machine Kills Secrets: How WikiLeaks, Cypherpunks and Hacktivists Aim to Free the World's Information*, 2012; Steven Levy, *Crypto: How the Code Rebels Beat the Government*, 2001; Peter Ludlow, ed., *Crypto Anarchy, Cyberstates, and Pirate Utopias*, 2001). No volume can hope to cover all the disparate disciplinary conversations about a particular phenomenon; however, this literature, the actors it considers, and the events it articulates are directly related to Egloff's work and the conceptual ground he is attempting to cover, making its exclusion a lost opportunity to increase his book's impact.

In contrast to Shires's and Egloff's political science approaches, O'Hara and Hall's *Four Internets* unpacks the sociotechnical systems that create different internets in different places. They focus their attention on networks, data, and modernity, looking to see how value structures related to communication are enacted through and shape different internets, creating fragmentation and potential ruptures. O'Hara and Hall argue that the global internet—or what is often generally referred to monolithically as “The Internet”—is actually a sociotechnical system maintained through international internet governance. They argue that this “Internet” is a key driver in the “development of modernity” and the shift from an Enlightenment-based modernity to what they call a “digital modernity” (p. 21). Within this “Internet,” O'Hara and Hall identify not one but four conceptual approaches to internet governance: the Silicon Valley model, the Brussels Bourgeois model, the DC Commercial model, and the Beijing Paternal model. They also include one other model that they treat as analytically different: the Russian Spoiler model. Finally, while they do not call it a model, they focus on India as a “swing state.” They argue that the models they examine are responses to this concept of digital modernity.

Unlike Shires or Egloff, O'Hara and Hall begin their analysis by articulating technical concepts for a lay audience. They start with a discussion of internet protocols (e.g., TCP/IP) to illustrate the “Internet's” essence as a global network connected using shared protocols that allow for the transfer of data. They illustrate that although these networks are designed to be decentralized, non-democracies find this design to be inherently threatening, causing such states to attempt to co-opt the “Internet” to enforce nondemocratic power structures. These different governance structures make a splintered set of internets more possible in the future.

Drawing on secondary sources focused on technology and writings that theorize or discuss political systems in different parts of the world, O'Hara and Hall then turn to the empirical work of the book beginning with their first

model of an internet: the Silicon Valley Open Internet. Here they argue that the model's form was shaped by many of its academic and libertarian-leaning creators who rejected state power. From this rejection, O'Hara and Hall point out that a range of actors have generated internet governance protocols and institutions and that this process has been reactive and ad hoc, based on solving pressing problems and evolving. The discussion of the Silicon Valley Open Internet is a rich but accessible look at the historical development of the global “Internet,” including key institutions (e.g., ICANN), and underlying logics (e.g., multi-stakeholderism). The discussion ends with Wikipedia, where O'Hara and Hall unpack the issue of how to govern while maintaining a vision of an open, nonhierarchical, democratic internet even when complex systems and disruptive actors create a management need for hierarchical bureaucracies.

The discussion of Wikipedia serves as the pivot point for O'Hara and Hall, leading them into their elaboration of the other models mentioned in the book's title. The first of the non-Silicon Valley models is the “Brussels Bourgeois” internet: an anticipatory model meant to calculate harms and neutralize them while embedding the preservation of human rights into its structure. O'Hara and Hall argue that, like the Silicon Valley model, this model is grounded in the preservation of openness, but it also privileges “civility and respect” (p. 83). The model is founded on what O'Hara and Hall argue is a different conception of political culture than the Silicon Valley model, and they use the European Union's approach to privacy, in particular its General Data Protection Regulation, to illustrate this approach.

The next model is the “DC Commercial” internet model—which the authors argue has been the driver of much innovation but at the cost of user privacy. O'Hara and Hall argue that this conceptualization of the internet is characterized by “closed networks, legitimate (i.e., not illegal, ideally contractual) barriers to market entry and network exit, and conditional tolerance of monopoly” (p. 105). This model posits that regulation should be minimal and government censorship avoided while private actors are allowed to determine content on their services. The DC model fosters the preservation of open standards at the internet level and transparency that is supported for commercial purposes such as stock trading, without much support for net neutrality (p. 106). While the Silicon Valley internet is also a US-based model, O'Hara and Hall argue that the Silicon Valley model expresses a US West Coast set of values, while the DC model is based on a US East Coast set of values.

O'Hara and Hall then articulate the Beijing Paternal model, a model in which the internet is “subordinate to centrally defined beneficial outcomes” (p. 126). They state that “paternalism” is a major characteristic “in Pacific Asia, Middle Eastern, and Latin American

cultures” (p. 126). The underlying idea is that a legitimate authority defines beneficial outcomes. O’Hara and Hall argue that China exemplifies this model, and they tie this to what they argue are Chinese values. For them, the Beijing model focuses on social stability and protection of the Communist Party’s power position, and works to ensure China’s position as a global power. They argue that Chinese internet policy focuses on directing the online environment, cybersecurity, national autonomy, and influence. O’Hara and Hall claim that it is the most divergent of the models with a heavy focus on control over all other factors.

O’Hara and Hall also include two other models that are not one of the four “internets” in the book’s title—the Moscow Spoiler model and the Indian Swing State model. The Moscow Spoiler model is built on the idea of subversion of existing models, what O’Hara and Hall call “plain vandalism” (p. 154). Problematically in light of the literature on hacker politics and hacktivism (Coleman 2012; see also Coleman, “Anonymous in Context: The Politics and Power behind the Mask,” *Internet Governance Papers*, 3, 2013), they explicitly tie the Moscow model to the ethic of hacking and hacker culture including hacktivism, articulating this as an adherence to “joy, creativity, and competitiveness,” pushing back on norms of behavior and other challenges to authority (p. 154). In terms of the Indian Swing State model, at the conclusion of the book, O’Hara and Hall discuss the “The Internet’s” future, which for them is captured in the Indian Swing State model. India is often referred to as a “swing state” in international internet governance debates, but here O’Hara and Hall specifically mean India in reference to the models that they have set forth in their book, examining Indian orientation to openness, commercialism, paternalism, and being a spoiler.

A major contribution that O’Hara and Hall’s book offers is their articulation of a set of ideal types —“internets” that offer analytical leverage for understanding global politics. Their conceptual framework is grounded in clearly communicated technical details, protocols, and nuances along with case studies that mean the book can serve as a starting point for someone new to

studies of the global internet. However, the book remains firmly glued to the Global North in terms of the “internets” articulated. The rest of the world, which has been generally underdiscussed and understudied in literature focused on the global internet and cybersecurity, remains peripheral. This has the unfortunate impact of putting the rest of the world in relation to the Global North while moving over ground that has been covered before. Other than through a problematic application of the idea of “paternalism” to the majority of the world, no other manifestations of internet governance are substantively discussed. The exceptions are the conceptual model of Russia as a vandal—with India discussed at the end in relation to its potential adherence to one of the other models. This leaves the majority of the world largely undiscussed, or appended onto one of the four internets, limiting the book’s contribution.

All three volumes reviewed here contribute in unique ways to the conversation about how to understand the global internet in relation to international affairs. When examined together, each offers an important model for the study of the internet in global politics. Shires’s inductive approach to understanding how cybersecurity is defined across many different groups offers one of the most holistic articulations of the interdisciplinary nature of the field I have read, and it is an approach that should be replicated. Egloff’s more narrow, but similarly impactful, focus on nonstate actors provides the field with a needed model for attacking one of the major analytical (and policy) issues in international cybersecurity. It also serves as an important reminder that although cybersecurity as a field is new to many, states’ interests have long been entwined with the interests of “pirates” of one sort or another. Finally, O’Hara and Hall’s work offers a view of internet infrastructures and the values and policies that shape them. As the field becomes more complex and moves past simpler understandings of cybersecurity as only involving major nation-state actors and destructive cyberattacks, these books offer not only important insights but also excellent frameworks for understanding this complex and emerging area of study for political science scholars.