COUNCIL on FOREIGN RELATIONS

The Failure of Academic Progress in Cybersecurity

Brandon Valeriano and Miguel Alberto Gomez

July 20th, 2020

During a recent cybersecurity workshop, a senior security studies scholar asked, “where are all the junior scholars? Who is producing the new PhDs?” Sadly, the answer is no one. Although there are isolated outposts of academic cybersecurity research and scholars making their own way, academic progress in cybersecurity from a social sciences perspective is lacking, and there remains no academic group for it at the major interdisciplinary international studies organization, the International Studies Association.

The social sciences play a significant role in illuminating the causes and consequences of cyber operations. The challenge to doing this is immense, as cybersecurity is an interdisciplinary field that requires more than just support from computer scientists and engineers, but also a firm grasp of international relations, law, criminology, psychology, and economics.

Unfortunately, the field of cybersecurity suffers from a lack of progress in the construction of a methodological framework and theoretical core. Moreover, there are only a few established scholars training doctoral candidates to conduct research. Those who do finish their degrees and find paid employment are often traveling blind with few guides on how to effectively publish in peer-reviewed outlets and contribute to policy discussions.

The Need for Research Methodologies

Currently, cybersecurity studies lack research methodologies and a consideration of epistemological outlooks. Without these, the field remains plagued by underdeveloped theories formed through speculation, lacks a foundation for analyzing empirical evidence connected to these theories, and fails to build on prior knowledge. While advances continue to be made in terms of the maturation of the field and the emergence of quality scholarship, this remains the exception, rather than the rule: there have been less than ten peer-reviewed cybersecurity publications in top-tier international relations journals over the last twenty years.

Geographic Blind Spots

Cybersecurity scholarship is also constrained by persistent geographical preferences. Despite the interconnected nature of the domain, a cursory examination of the literature reveals an implicit dichotomization between American and European cyber scholarship focusing on a narrow set of cases, namely Iranian and North Korean cyber activity, and a concerning dearth from other regions, such as Asia-Pacific and Latin America, where interest in cybersecurity is growing. Until there is greater representation from these regions, cybersecurity research will be limited by its narrow geographic scope.

Theoretical Guidance and Policy Relevance

Aside from these methodological shortcomings, Cybersecurity also lacks theoretical guidance to complement the collection of empirical evidence, such as data regarding cyber activity, and explain what drives behavior in cyberspace.

On the other extreme, the notion that the novelty of cyberspace requires the reinvention of theoretical frameworks, such as deterrence theory, is equally problematic. Behavior in cyberspace is motivated by the same factors that influence other actions in the international arena. Although the medium often requires us to reconceptualize and adapt prior theories of interstate behavior, they are still useful and should not be discarded.

The lack of progress in the development of cybersecurity as an academic field inevitably hinders the policy relevance of cybersecurity research. Although influencing policy is not always the goal of academic research, such a claim is dubious for cybersecurity because it has direct policy implications. A continued shortage of cybersecurity expertise has caused policymakers to seek out superficial contributions that lack empirical evidence and even derive inspiration from fiction on occasion.

We Need Mentors

Ultimately, these gaps reflect issues in mentorship provided to doctoral students. While it is easy to blame poor mentorship on individual idiosyncrasies, structural factors also play a significant role in this regard. For example, the tendency of academic cybersecurity research to be Western-centric could result in a narrowed view of the field among those guiding young scholars in other parts of the world. Also, the failure to recognize cybersecurity's interdisciplinary nature limits collaborative work between emerging and senior scholars across different disciplines. These issues consequently limit academic progress.

There are, fortunately, reasons to be optimistic about the future of the field. Interdisciplinary journals, such as the *Journal of Cybersecurity* and the *Journal of Cyber Policy*, have emerged and maintained credibility over time, and book publishers are hungry for academic takes on the challenge of cybersecurity. In addition, cybersecurity scholars are taking the initiative to establish forums, such as the *Digital Issues Discussion Group*, where new research is scrutinized outside existing geographical or disciplinary confines. Similarly, a handful of institutional fora have been created to facilitate the exchange of academic cybersecurity research and best practices between scholars.

The advancement of cybersecurity as an academic discipline requires us to step away from a siloed approach to research and recognize the need for strong social science research in the field. This should be combined with the analysis of less familiar but significant events in cyberspace, expanding existing theory in new directions, and collaboration that transcends disciplinary boundaries. The benefits of addressing these challenges are well worth the effort to cultivate cybersecurity as a growing and critical field of study.

Brandon Valeriano is the Bren Chair of Military Innovation at the Marine Corps University. He also serves as a senior fellow at the Cato Institute and a senior advisor for the Cyberspace Solarium Commission.

Miguel Alberto Gomez is a senior researcher with the Center for Security Studies at the Swiss Federal Institute of Technology. He is also a doctoral candidate at the Universität Hidesheim.