Texas National Security Review: Volume 3, Issue 4 (Fall 2020)
Print: ISSN 2576-1021 Online: ISSN 2576-1153

THE DYNAMICS OF CYBER CONFLICT AND COMPETITION

Robert Chesney

Max W. Smeets

In the introduction to our special issue on cyber competition, guest editors Robert Chesney and Max W. Smeets challenge the way in which cyber attacks and cyber competition are often studied and explain why they felt an "intervention" was needed.

Cyber attacks seem to have become natural, necessary, and normal. Nearly every day, mainstream media is filled with reports of hacks, leaks, cyber espionage, and other attacks perpetrated through and in cyberspace. A diverse group of states across the world claim that they are exploring options to further develop an offensive cyber capacity. Nonstate actors continue to rely on cyber means while pursuing a diverse set of motives.

Despite this ubiquity, the dynamics of cyber conflict and competition are complex, understudied, and constantly changing. In 2010, Keith Alexander appeared before the Committee on Armed Services in the U.S. Senate to review his nomination to become the first commander of the U.S. Cyber Command and lead the National Security Agency. He stated that there is "much uncharted territory in the world of cyber-policy, law and doctrine."[1] Alexander's statement still holds today.[2]

Uncertainty pervades a broad set of cyber issues, including the potential normative restraints in cyberspace, the viability of export controls, the strategic value of cyber operations, and the ways in which state and nonstate actors can and do cooperate — both from an offensive and defensive perspective. Researchers have tried to answer these questions while the conceptual and empirical underpinnings of the field are fluid. New "data points," like the cyber-enabled information operations during the 2016 U.S. presidential election, have frequently shifted the focus of the field and changed our understanding of what cyber conflict and competition entails. New interpretations of old data points, like the study on the 1990s Moonlight Maze campaign, have also altered our understanding of the field.[3]

The purpose of this special issue is to push the field of cyber studies forward, by bringing together contributions from scholars and practitioners. We see this issue less as a survey of the field and more as an intervention. We believe this intervention is welcome for at least two reasons. First, while new material is published on a daily basis, we can hardly say that the field is saturated with rigorous theoretical and empirical analysis.[4] In his classic work *Strategies of Containment*, John Lewis Gaddis divides historians into two groups: lumpers and splitters. Lumpers seek to find patterns in past events and "reduce the chaos, disorder, and sheer untidiness of history." The ultimate goal is to provide broad generalizations through systematizing the complexity of long epochs or events. Splitters, in turn, "point out exceptions, qualifications, incongruities, paradoxes."[5] For the field of cyber conflict and competition, we need both more lumpers and more splitters — and especially those who can strike a delicate balance between the two.

Second, we believe the borders of the field of cyber conflict and competition require realignment. Silos of research — the internal borders — are emerging within the field, but we believe that these are not always helpful. For example, cyber conflict scholars rarely interact with the digital governance community. A dialogue between the two fields would help in better understanding opportunities for cyber stability. Equally, though there

1 Keith Alexander, Testimony to the U.S. Senate, Committee on Armed Services, quoted in Brian Prince, "NSA Director Says Cyber Command Not Trying to Militarize Cyberspace," *eWeek*, April 15, 2010, http://www.eweek.com/security/nsa-director-says-cyber-command-not-trying-to-militarize-cyberspace.

2 Similar statements were provided by Vice Adm. Michael S. Rogers in 2014 and Lt. Gen. Paul Nakasone in 2018. U.S. Senate Armed Services Committee, "Advance Questions for Vice Admiral Michael S. Rogers, USN Nominee for Commander, United States Cyber Command," March 11, 2014, 7–8, www.armed-services.senate.gov/imo/media/doc/Rogers_03-11-14.pdf; U.S. Senate Armed Services Committee, "Stenographic Transcript before the Committee on Armed Services United States Senate Nominations for Lieutenant General Paul Nakasone to be Commander of the U.S. Cyber Command and Director of the National Security Agency and Chief of the Central Security Service," March 1, 2018, https://assets.documentcloud.org/documents/4407097/United-States-Senate-Armed-Services-Committee.pdf.

3 In this case, the research of Kaspersky Lab, Dan Moore, and Thomas Rid revealed how actors can evolve over time and revealed the potential longevity of cyber campaigns. Kaspersky Lab, "Moonlight Maze: Lessons from history," *Kaspersky Daily*, April 3, 2017, https://www.kaspersky.com/blog/moonlight-maze-the-lessons/6713/.

4 For a systematic review of political science scholarship on cyber conflict and competition, see, Robert Gorwa and Max Smeets, "Cyber Conflict in Political Science: A Review of Methods and Literature," *Working Paper for the 2019 International Studies Association Annual Convention*, Toronto 2019, https://doi.org/10.31235/osf.io/fc6sg.

5 John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War, Revised Edition* (New York: Oxford University Press, 2005), vii.

could be advantages to seeing the field of cyber conflict studies as distinct from other areas, we believe that a further push outward toward other areas of research, such as computer science and intelligence studies — the external borders — is beneficial to better capturing the dynamics of cyber conflict and competition.

This intervention in the field is timely given the current policy climate on cyber security. Over the past few years, the U.S. government has undergone a shift in strategic thinking of a kind that we have not seen since the 1990s, if ever.[6] The move away from the anchoring concepts of deterrence and resilience toward persistent engagement and "defend forward" is significant for how the cyber environment is perceived and shaped, how threats are counted, and how resources are allocated.[7] Equally, other countries such as France and the United Kingdom are reconsidering their cyber policy efforts.[8] At a time of fundamental policy changes, it becomes especially important to rethink the parameters of the field that underlie it.

IN THE FUTURE, WE MAY NO LONGER TALK ABOUT "CYBER CONFLICT," BUT INSTEAD SIMPLY DISCUSS "CONFLICT," KNOWING THAT THE LINES SEPARATING ONE FROM THE OTHER HAVE BECOME ESSENTIALLY INVISIBLE.

Our ambitions, our conception of cyber conflict and competition as a field of study, and the current policy climate have all shaped the structure and contents of this special issue. The articles — especially in the Scholar section — seek to both advance theoretical interpretations and bring in new empirics. James Shires widens the empirical basis of debates around hack-and-leak operations and argues that such operations are the "simulation of scandal," or in other words, "deliberate attempts to direct moral judgment against their target." Ben Buchanan and Fiona Cunningham analyze Chinese and U.S. leadership views, organization setup, and bilateral relations to provide new insights on the risk of inadvertent escalation between the two great powers.

Second, despite strong differences in the field, many of us are concerned about how we should form policy. The policy dimensions of the cyberspace debate are directly addressed in the Strategist section of this special issue. Emily Goldman illustrates how the U.S. State Department should alter its current norms and deterrence posture and operationalize cyber persistence. Goldman thoughtfully lays out seven recommendations that serve to push U.S. cyber diplomacy in the right direction. Kim Zetter examines the election security crisis and discusses the need for software-independent solutions and state election laws. We have also asked authors to explicitly spell out the policy dimensions of their scholarly contribution. Jason Healey and Robert Jervis' assessment of the conditions under which cyber capabilities are escalatory — found in the Scholar section — draws out important lessons for stability. The article explains the need to reduce one-sided knowledge about cyber activity and measurement and delineates the limits of norm-building projects.

Third, we have sought to make sure the scholars directly speak to each other on these fundamental questions facing the field of cyber conflict and competition. This is most evidently provided in the policy roundtable, exploring whether cyber conflict might be understood as a form of intelligence competition. But it also applies to other articles in this issue. Indeed, Goldman's Strategist piece on the need for a new course for U.S. cyber diplomacy pairs well with Healey and Jervis' as well as Buchanan and

6 Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5, no.1 (2019): 1–15, https://doi.org/10.1093/cybsec/tyz008. For works on the early 1990s shift in thinking, see, Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon and Schuster, 2017); Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Washington DC: Cyber Conflict Studies Association, 2013).

7 U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command*, March 2018, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf; Richard J. Harknett, "United States Cyber Command's New Vision: What It Entails and Why It Matters," *Lawfare*, March 23, 2018, https://www.lawfareblog.com/united-states-cyber-commands-new-vision-what-it-entails-and-why-it-matters.

8 Francois Delerue, Alix Desforges, and Aude Gery, "A Close Look at France's New Military Cyber Strategy," *War on the Rocks*, April 23, 2019, https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/. Having said that, most NATO members still devote very limited resources to build up a military cyber capacity. See, Max Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," *9th International Conference on Cyber Conflict* (NATO CCD COE: 2017), https://ccdcoe.org/uploads/2019/06/Art_09_NATO-Members-Organizational-Path.pdf.

Cunningham's articles on escalation risks.

To paraphrase Ian Wallace, there was a time when we talked about the "digital economy." Now, we just talk about the "economy." In the future, we may no longer talk about "cyber conflict," but instead simply discuss "conflict," knowing that the lines separating one from the other have become essentially invisible.

Ultimately, we hope this special issue will not only inform old debates and start new ones in the field of cyber security, but will also be valuable to the wider international security community. After all, it has become increasingly difficult to disentangle the two. We would like to thank the authors for their contributions, the reviewers for improving the quality of the manuscripts, and the editorial staff at *Texas National Security Review* for their help in the production of this special issue. We would also like to acknowledge the financial support of the Hewlett Foundation for this project through the University of Texas. We hope you enjoy reading the articles as much as we enjoyed editing them. ♜

Robert Chesney *is the James A. Baker III chair and associate dean for academic affairs at the University of Texas School of Law. He also serves as director of the university's Robert S. Strauss Center for International Security and Law and is the author of the free interdisciplinary casebook* Chesney on Cybersecurity Law, Policy, and Institutions (*available via the Social Science Research Network*). *He is one of the co-founders of* Lawfare *and is co-host of the weekly show* The National Security Law Podcast.

Max Smeets *is a senior researcher at the Center for Security Studies (CSS). He also serves as the director of the European Cyber Conflict Research Initiative (ECCRI). Max is an affiliate at the Stanford University Center for International Security and Cooperation and research associate at the Centre for Technology and Global Affairs, University of Oxford.*