# Introduction: An Offensive Future?

Dr. Andrew C. Dwyer
Dr. Amy Ertan

The recent cyberattacks against Colonial Pipeline and Solar Winds in the United States, the Health Service Executive in Ireland, and extensive and ongoing cyber activity in Ukraine highlight the continuing threats and complex security needs of our interdependent societies. Such operations and attacks are conducted by states that do not claim to possess offensive cyber capabilities, such as Russia and China, or by sophisticated cybercriminal gangs who commonly deploy ransomware, particularly with "hack and leak" operations, to generate an enormous amount of revenue. In response, many states have developed cyber capabilities to address the growing insecurity of states, their citizens, and various communities, with varying degrees of success and organization.[1] Thus, as states have been establishing more assertive responses to malicious cyber activities through offensive cyber forces or units of their own, there has been a concurrent development of connecting this with broader cyber security, resilience, and capacity building, often around the pursuit and projection of cyber power.

In this special issue of *The Cyber Defense Review*, the contributing authors were asked to explore the contours of living in a future world where there is more explicit activity, and public recognition of, offensive cyber operations and the key issues that need to



1 Max Smeets, *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (London: C Hurst & Co Publishers Ltd, 2022), and for a discussion on the UK, see Joe Devanny et al., "The National Cyber Force That Britain Needs?" (London: King's College London, April 21, 2021), https://www.kcl.ac.uk/policy-institute/assets/the-national-cyber-force-that-britain-needs.pdf.

**Dr. Andrew C. Dwyer** is an Addison Wheeler Research Fellow at Durham University (Durham, UK) in its Department of Geography. His research covers technological decision-making, offensive cyber policy, as well as creative approaches to the study of cybersecurity. He is Co-Lead of the Offensive Cyber Working Group and in Fall 2022 will be an Assistant Professor in the Information Security Group at Royal Holloway, University of London.

be considered. Such a process suggests that the need for attentiveness is not only limited to military and strategic spheres and recognizes that cybersecurity and cyber power must be maturely and appropriately understood. Offensive cyber operations must consider social, cultural, political, and economic interests together with civil society, private businesses, and academia, which some states call a whole-of-society approach. Thus far, there has been a limited analytical focus on such a critical and broad interpretation of offensive cyber activities, which this special issue seeks to address. By considering what an "offensive future" may look like, as guest editors, we do not define offensive cyber nor take a position on its future use as different communities will interpret this differently. We instead note that offensive cyber activities are already part of our present and have developed considerably upon older practices of intelligence and effects operations, as much as their effects are felt unevenly. Therefore, we present a set of thought-provoking articles examining this nascent discussion, with its contested definitions and contours, and offer insights into numerous practices and implications across three primary themes.

In the first theme, there is an exploration of some of the economics that underpin both the capacity to engage in offensive cyber operations through an analysis of exploits as well as the implications for societies that may be the target of such actions. Kicking off the special issue, in "Prepare and Prevent, Don't Repair and Repent: The Role of Reinsurance in Offensive Cyber," Alicia Bates explores the power of resilience and argues for the need for a new framework of cyber insurance that accounts for offensive cyber activity. In so doing, the paper argues that a reinsurance framework may reduce the risks and unintended consequences of offensive cyber operations and thus a state's capac-

**Dr. Amy Ertan** is a cybersecurity fellow at the Harvard's Belfer Center for Science and International Affairs, cyber strategy researcher at the NATO Cooperative Cyber Defence Centre of Excellence. She received an Information Security doctoral degree from Royal Holloway, University of London. Her research focuses on cyber conflict and the security implications of emerging technology, and she is the co-lead of the Offensive Cyber Working Group. Amy's recent co-authored publications include the NATO CCDCOE report: "Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment" and the *King's Policy Institute Report:* "The National Cyber Force that Britain Needs?" She holds CISSP and CRTIA qualifications and has previously worked in cyber-wargame scenario design, human factors cyber security research and strategic cyber intelligence.

ity to deliver an offensive strategy that can receive a more positive reception from its publics. In exploring the technical capabilities of conducting operations, Matthias Dellago, Dr. Daniel Woods, and Dr. Andrew Simpson examine broker quotes for cyber exploits from those who claim to sell to government actors in "Exploit Brokers and Offensive Cyber." Their analysis informs our understanding of supply and demand for offensive cyber capabilities in private markets, and the transforming economies of exploits.

In a second theme, authors paid attention to how offensive cyber is organized, approached, and constructed. During a time when there are different, competing visions of the future of the Internet, in "Democracies and the Future of Offensive (Cyber-Enabled) Information Operations," Dr. Bryan Nakayama analyzes how Western democracies have responded to cyber-enabled information operations, and concludes that democracies should avoid practicing such offensive operations entirely in an alternative perspective on what our future should be. Moving to a focus on organizations, in "Between Two Stools: Military and Intelligence Organizations in the Conduct of Offensive Cyber Operations," Dr. Ewan Lawson carefully details how the organizational context in which offensive cyber capabilities operate are blurred between intelligence agencies and the military. This research argues that such a blurring is problematic as it both contributes to unintended escalation between states and increasing the potential for destructive "grey zone" activity below the threshold of war, with implications for the application of international humanitarian law (IHL). Dr. Nori Katagiri continues this conversation by examining when the conduct offensive cyber operations is an appropriate and required course of action, and proposes a set of criteria in "Three Conditions

for Cyber Countermeasures: Opportunities and Challenges of Active-Defense Operations," alongside detail on associated challenges in meeting each of the proposed conditions.

After exploring economics, organization, and construction, the third theme of this special issue offers two pervasive perspectives on the narratives and assumptions on offensive cyber activity. In "The Failure of Offense/Defense Balance in Cyber Security," Dr. Brandon Valeriano highlights the pitfalls in the attempts to apply the principle of an offense/defense balance to research. In so doing, he identifies a "strategic malaise" resulting from a mistaken approach in assuming that the advantage always lies with the attacker. In comparison, Dr. Joe Burton explores the diverse academic approaches to cyber conflict in "The Future of Cyber Conflict Studies: Cyber Subcultures and The Road to Interdisciplinarity," which highlights the power of interdisciplinary scholarship to enable more holistic and nuanced debates and understandings of the field's dynamics. He draws from International Relations, Political Psychology, International Law, and Computer Science to explore the intricacies, mistranslations, emphases and contributions of each.

Dr. Rod Thornton and Dr. Marina Miron then close out the issue as they explore how Russia thinks through the power of cyber capabilities and their potential to generate strategic outcomes in "Winning future wars: Russian offensive cyber and its vital importance in Moscow's strategic thinking." This is demonstrative of a broader approach to strategic thinking where the country sees itself at a strategic disadvantage to NATO in other arenas of warfare. Both authors also offer some early reflections in relation to the ongoing war in Ukraine, demonstrating some of the differences between Western and non-Western conceptualizations of offensive cyber in the 21st Century.

We hope that these papers—variously covering economics, organization, strategy, and the case of Russia—offer avenues to broaden the scope of discussion on offensive cyber activity and its interdependencies with cyber security and cyber power. Each paper adds something new to the discussion, helping to address the urgent need for more nuance in this space. There is, however, a need for further debate that goes well beyond the scope and generosity of these eight papers. This debate ought to explore emerging and disruptive technological trends, examine international relationships beyond the usual suspects of "great" power competition between the US, China, and Russia as well as the role of "second-tier" powers including the UK and France. Similarly, conversations must take place at all levels, from exploring organizational contexts to clarifying processes around oversight and talent, to discussions on international norms and deterrence theory. While this special issue explores several of these themes, efforts to disentangle these themes and subjects are needed more than ever. We therefore see this as an open invitation to deepen and extend the conversation. The Offensive Cyber Working Group—which we co-lead and under which these papers were curated—will continue to promote conversations on these themes and welcomes engagement from research and policy communities to do so.

Finally, we thank all the contributing authors for their time and expertise for this issue. We are particularly grateful to Dr. Corvin Connolly and the editorial team at *The Cyber Defense* Review, who have been incredibly supportive throughout the entire publication process. It has been a pleasure.