H-Diplo Review Essay 315

19 February 2021

Scott Jasper. ***Russian Cyber Operations: Coding the Boundaries of Conflict.*** Washington, D.C.: Georgetown University Press, 2020. ISBN 978-1-62616-797-1 (hardcover, $32.95).

https://hdiplo.org/to/E315
Editor: Diane Labrosse | Commissioning Editor: Michael A. Innes | Production Editor: George Fujii

Review by Tim Stevens, Dept. of War Studies, King's College London

Russian Cyber Operations is an in-depth exploration of how Russia exploits computer networks to promote its strategic ambitions against its adversaries. We are now well-acquainted with expressions like 'cyber attack' and 'cyber-enabled information operations,' even as these terms are often misunderstood or misused in public discourse. Whether this book will demystify what they are is moot on account of the preponderance of technical jargon, even if Scott Jasper is a better translator than some, but it does explain why Russia deems them desirable and how they nestle within its wider strategic vision and self-identity. Ultimately, though, this is a book about the United States. The stated purpose of the book is to promote a specific set of countermeasures that automate U.S. cyber defences against a sophisticated and determined foe like the Russian Federation. It therefore marries a detailed historical narrative of Russian cyber aggression with a limited programme for U.S. organisational adaptation and perspectival change.

The first part of the book concerns itself with "Cyber Operations," describing in rich empirical detail three variants of Russian computer network operations in recent years: as asymmetric 'cyber warfare,' as a component of 'hybrid warfare,' and as part of the wider Russian practice of 'information warfare.' Much of this will be familiar to readers in the field, especially the case studies of Estonia (2007) and Georgia (2008), as well as the Democratic National Committee 'hack-and-leak' operations during the 2016 U.S. Presidential elections. However, these chapters synthesise well a diverse range of primary and secondary sources; each provides a robust report of the phenomena under review and, importantly, locates them firmly within Russian strategic thinking on sub-threshold conflict.

The general reader should find these of use, as will researchers who are looking for authoritative and well-bounded accounts of how Russia has used its national cyber capabilities in peace and in war. Of particular interest is the sometimes startling tale of Russian cyber operations against Ukrainian army units since 2014 (62-63), which demonstrates just how effective – and imaginative – such campaigns can be, especially when combined with Russia's substantial electronic warfare capabilities as part of an integrated projection of military force and non-military informational measures. In addition, each chapter addresses the legal status of Russian cyber operations in international law. These sections are not quite a systematic application of the "Analytical Framework" set out in Chapter One, but they do serve as helpful, if brief, reviews of legal opinion on various operations, albeit ones which lean heavily on U.S. sources and the NATO-sponsored *Tallinn Manual* process.[1] To be scrupulously fair to the author, there are few international legal texts like the *Tallinn Manuals*, let alone any that are as comprehensive or that have involved diverse stakeholders during their consultative phases. Nevertheless, one wonders how non-Western legal scholars and jurists may have interpreted these events.

[1] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013); Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge: Cambridge University Press, 2017).

© 2021 The Authors | CC BY-NC-ND 3.0 US

The aim of these empirical chapters is fourfold. First, to show that Russia's grand strategy is "to restore its status as an independent great power" (3) and that all other considerations are subservient to this. Second, to establish that Russia is a bold and highly capable actor in cyberspace, as demonstrated in the case studies. Third, that Russian military doctrine and associated intelligence activities do not make the distinction between military and non-military, or between 'cyber' and 'information,' as the U.S. and its western allies do. These are uncontroversial propositions and Jasper's book does not seek to compete with, for instance, recent work by Ofer Fridman on hybrid warfare, or Keir Giles on Russian grand strategy.[2] Rather, it builds on these and other scholars to make points about the utility, specifically, of cyber operations to Russia and the subsequent reaction by the U.S. and its NATO allies. Crucially, as Jasper sets out in Chapters 5 and 6, which examine Russia as a rational strategic actor and the 'unconvincing responses' of the US to Russian provocation, respectively, the U.S. is failing to deter Russian cyber operations.

The inability of the U.S. to deter cyber aggression and the factors contributing to it have been discussed elsewhere, including in an earlier book by Robert Mandel.[3] The folly of pursuing cyber deterrence at all has been asserted most forcibly by Richard Harknett and Michael P. Fischerkeller.[4] Harknett and Fischerkeller are in the unusual position of having influenced U.S. doctrine to such a degree that their proposals for 'persistent engagement' have been translated into U.S. military cyber strategy.[5] As Jasper notes, this shift in posture portends more proactive operations in non-permissive environments outside U.S. networks, in which, as the former deputy commander of U.S. Cyber Command, Lt. Gen. Vincent Stewart, argued, the U.S. will "impose cost on their [the enemy's] behavior and make sure that we are going to shape norms and behavior in this space" (131). Accompanied by organisational changes and legal authorities under the administration of President Donald Trump, persistent engagement was meant to renew deterrence in cyberspace by reinforcing U.S. credibility and capability. Unfortunately, asserts Jasper, it has done nothing of the sort. Like other liberal democracies, the U.S. is not keen on responding strongly to cyber operations below the threshold of conventional force; it is also worried about escalation. As a result, rather than signalling to Russia that "cyber operations will not be tolerated … Russia continues to conduct cyber operations without fear of reprisal" (132).

The rest of the book details how to remedy this situation. Jasper's previous book dealt with "active cyber defense," which he defined as "the real-time detection, analysis, and mitigation of network security breaches combined with the aggressive use of countermeasures beyond network and state territorial boundaries."[6] Persistent engagement addresses the latter part of this equation, as it operates outside US sovereign borders, albeit in a dubious legal space. The ambition to impose costs on adversaries, achieving deterrence by punishment, is what is failing. Jasper asks us to look again at deterrence by denial – the first part of the active cyber defence proposition – whereby adversaries' behaviours are altered as they learn that their actions cannot succeed against robust cyber defences. The principal pitch here is that the defensive tools deployed under existing cyber risk management frameworks are ill-equipped to deter an adaptable foe like Russia. They are too slow and inflexible. The solution proffered is that the U.S. should automate its cyber defences via an approach to Russian threat actors that is "proactive, adaptable, and, most important, resilient" (157).

---

[2] Ofer Fridman, *Russian Hybrid Warfare: Resurgence and Politicisation* (New York: Oxford University Press, 2018; Keir Giles, *Moscow Rules: What Drives Russia to Confront the West* (Washington, D.C.: Brookings Institution Press, 2019).

[3] Robert Mandel, *Optimizing Cyberdeterrence: A Comprehensive Strategy for Preventing Foreign Cyberattacks* (Washington, D.C.: Georgetown University Press, 2017).

[4] Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis* 61:3 (2017): 381-393, DOI: https://doi.org/10.1016/j.orbis.2017.05.003.

[5] US Department of Defense, *Summary: Department of Defense Cyber Strategy 2018*, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[6] Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Lanham: Rowman and Littlefield, 2017), 165.

© 2020 The Authors | CC BY-NC-ND 3.0 US

From the perspective of most of the cybersecurity industry and of government agencies charged with cybersecurity, this is a sensible proposal. Automation routinizes cyber defence and frees up human resources to tailor responses to high-end criminal and strategic actors. If systems are set up to adapt over time through machine learning and advanced data analytics, they can provide a more efficient and effective response to anomalous behaviours that are identified in the networks. Deployed properly, they can also provide network 'defence-in-depth' that is not afforded by existing approaches. The problem for this book is that this is already a standard, if not wholly established, way of thinking about network defence. Indeed, as the author shows, a proprietary system has been installed at his own workplace; much of Chapter 8 describes this and other products in some technical detail.

These sections are seemingly not intended for non-specialists, given sentences such as "the DLL File Protection Module would block the injected dynamic link library (DLL) payload (containing embedded ransomware) from starting the encryption process and lateral movement" (175). It is also questionable whether an academic volume should promote named software products, as this book seems to do, without any recognition that it might be doing so (171-176). Moreover, the whole register of the book appears to shift in Chapter 8. In the earlier part of the book, technical details are interwoven tightly with the strategic narrative; here the author dives into the tactical and the operational aspects of organisational cybersecurity, whereby the strategic becomes somewhat obscured by the technical. It is not obvious how 'automated cyber defense' should be used to address national cybersecurity concerns above the level of the agency or the firm, although the book concludes with a call that these forms of cyber defence-in-depth should be an integral part of the U.S. Third Offset Strategy that was announced in 2014 and is currently awaiting full adoption.

In common with most mainstream U.S. works on cybersecurity, Jasper's book does not look far beyond the U.S. itself. The occasional mention of NATO is not accompanied by any developed consideration of the implications of U.S. cyber posture for NATO allies and partners. This reflects the emphasis of American scholarship and commentary on persistent engagement generally, which only rarely acknowledges the relevance of other non-adversarial relationships to U.S. decision-making.[7] This parochialism extends to most Western authors in the field, most of whom are fixated on great power competition and all but ignore small states or those in the global South. How, for example, states with less influence and fewer resources than the U.S. might adopt automated cyber defence systems is not addressed, nor is their fate should they be unable to do so.

Russian Cyber Operations is not aimed to satisfy readers who are looking for theoretical advancement in the fields of cybersecurity, cyber conflict, cyber strategy or, indeed, International Relations or strategic studies. The book is meant as an open policy intervention that seeks to persuade the U.S. to adopt automated cyber defence and therefore improve its capacity to deter an emboldened Russia. It provides some solid empirical case studies of Russian cyber operations and their strategic context, as well as useful reviews of U.S. legal and strategic responses and their shortcomings. Whilst at times the technical detail may seem misplaced, these sections can be skated over without any detriment to the overall argument, and both general and specialist readers will find much sustenance within.

Tim Stevens is Senior Lecturer in Global Security in the Department of War Studies, King's College London, UK. He has published widely on cybersecurity and related topics, including the monograph, *Cyber Security and the Politics of Time*, which was published in 2016 by Cambridge University Press.

[7] Max Smeets, "US Cyber Strategy of Persistent Engagement and Defend Forward: Implications for the Alliance and Intelligence Collection," *Intelligence and National Security* 35:3 (2020): 444-453. DOI: https://doi.org/10.1080/02684527.2020.1729316.

© 2020 The Authors | CC BY-NC-ND 3.0 US