Journal of Strategic Security

Volume 14 | Number 1 Article 8

Russian Cyber Operations: Coding the Boundaries of Conflict. By Scott Jasper. Washington, DC: Georgetown University Press, June 2020. ISBN: 978-1-626-16797-1. Hardcover. 232 Pages. $32.95

Chris Bronk
University of Houston, rcbronk@central.uh.edu

pp. 122-124

Recommended Citation
Bronk, Chris. "Russian Cyber Operations: Coding the Boundaries of Conflict. By Scott Jasper. Washington, DC: Georgetown University Press, June 2020. ISBN: 978-1-626-16797-1. Hardcover. 232 Pages. $32.95." *Journal of Strategic Security* 14, no. 1 (2020) : 122-124.
DOI: https://doi.org/10.5038/1944-0472.14.1.1925
Available at: https://scholarcommons.usf.edu/jss/vol14/iss1/8

Russian Cyber Operations: Coding the Boundaries of Conflict. By Scott Jasper. Washington, DC: Georgetown University Press, June 2020. ISBN: 978-1-626-16797-1. Hardcover. 232 Pages. $32.95

***Russian Cyber Operations: Coding the Boundaries of Conflict*. By Scott Jasper. Washington, DC: Georgetown University Press, June 2020. ISBN: 978-1-626-16797-1. Hardcover. 232 Pages. $32.95**

Reviewed by Chris Bronk, University of Houston

Did the National Security Agency, Cyber Command, and the Cybersecurity and Infrastructure Security Agency succeed in blunting Russian attempts to manipulate the U.S. 2020 national elections? It may take some time to have a clearer picture of what happened, and there have many fingers pointed in Vladimir Putin's direction, but as of February 2021, it appears that the U.S. government did a good job. But the Russians have made much mayhem in cyberspace, the SolarWinds cyber incident being yet another reminder of the Kremlin's significant capacity for digital espionage. Scott Jasper's superb *Russian Cyber Operations* provides an appraisal of just what the Russians have done, what they may attempt, and how different socio-technical approaches employed by the U.S. and its allies can do to reverse activity that does not necessarily rise to the level of military hostilities.

Captain Jasper (USN ret'd) has produced a qualitative study that rests upon understanding of different but interwoven cyber issues for national security policy beginning with the Law of Armed Conflict, asymmetric capabilities, and information and hybrid warfare. His consideration of other dynamics in cybersecurity and related information operations and activities, leveling more than a few critical points on U.S. responses to Russia's information confrontation (*informatsionnoye protivoborstyo*). The final portion of Jasper's book addresses new options for policy and technology that may prevent Russia from repeating what I would characterize as cyber successes either in combination with kinetic forms of conflict or absent military violence.

Handling the thorny question of when actions by bytes may necessitate response by bombs, in his analytic framework, Jasper asserts, quite correctly in my opinion, that "For cyber operations to satisfy the armed criteria of armed conflict, they would have to result in injury or death of persons or damage or destruction of property." His coverage of international law and norms regarding cyber conflict leads him to a likely

controversial claim that, "a solid international legal framework exists to govern how the United States and other countries should respond to cyber operations." This does not necessarily boil down to rules of warfare, but rather ones related to conflict, which is an evolving concept, not one frozen and clearly codified.

If there is one thing Russia has done, it is to produce an ample number of cyber cases, including: Estonia (2007), Georgia (2008), Ukraine power grid (2015), and NotPetya (2017). Much can be learned from Russia's behavior in its near abroad of former Soviet Republics. "Russia prefers to test the thresholds of armed conflict, using cyber operations and other ambiguous means in its asymmetric arsenal in continual 'day-to-day' competition with the United States and its allies," he argues. This assertion is demonstrated via cases tied to effective framing throughout the diagnostic sections of *Russia Cyber Operations*.
Coverage of both information and hybrid warfare is conducted with nods to both Russian strategic thinking and action. This includes a treatment of the 'Gerasimov Doctrine' as well as its application in analyzing the annexation of Crimea by Russian forces in 2014. Actions by Russian military units already based there as well as arrivals from outside were bolstered by cyber actions motivated by a desire to further, "disrupt and destabilize Ukraine." With this case, Jasper shows, as with the matter of cyber action against Georgia in 2008, how cyber activity can be part of a hybrid warfare strategy that employs force in actions that may not rise to the level of outright military hostilities.

Attention to information warfare, in the form of Russian broad conceptualization of how, "Cyber-enabled information operations give Moscow a covert means," to influence public opinion, organize protests, and reduce the will of its opponents to resist. It is here that Jasper throws light onto Russian doctrinal understanding of how information confrontation can be used to influence by "informational-technical effect," or "information-psychological effect." Russia clearly has a strong command of information operations and how they may be employed across a continuum of international affairs, both below and above the threshold of armed conflict. The information warfare concept is applied to the 2016 U.S. Presidential election, with the facts of the case concise and completely valid in the reviewer's opinion.

https://scholarcommons.usf.edu/jss/vol14/iss1/8
DOI: https://doi.org/10.5038/1944-0472.14.1.1925

There is an interesting pivot into the topic of "Rational State Behavior," which highlights how Russia has maneuvered around Western strengths in law and norms to achieve its goals, despite modest resources. Russia has done what it believes it can get away with through employment of cyber covert action and Jasper believes it will continue to do so. He is tough on U.S. policy responses to Russia thus far. Recent White House and DoD policy announcements regarding cyber action still have yet to "rebuild eroded credibility" as a convincing response to Russian activity. Indeed, Jasper argues, "the United States has failed so far to reintroduce the belief in Russia that malicious cyber operations will not be tolerated."

Having identified the issues regarding Russia's employment of cyber operations and the failures in U.S. and Western response to them, Jasper moves to a set of strategies and frameworks commonly identified in industry and government. This chapter feels, much its subject matter, ambitious, but not up to the task of meeting Russian cyber forces head on. Recent cyber incident case studies have employed the MITRE ATT&CK framework, which can be used to clearly identify points of cybersecurity failure in an organization. Jasper sees it as one of the mechanisms to providing drilled or automated response to cyberattack. He also eschewed the hype on artificial intelligence for a reasonable, straightforward treatment of how machine learning may aid in cybersecurity efforts.

I offer a high-level critique of Prof. Jasper's characterization of the Russian threat as I remain unconvinced that it will be an enduring one. While Russia's mastery of cyber/information operations is strong, it stands on the weakest of economic foundations. E.H. Carr's pre-World War II assessment of power encompasses a blend of military, informational, and economic ingredients. Setting aside the considerable internal dissent surrounding Alexei Navalny's populist campaign, Russia has the shakiest of economic footings as energy exports stand at the center of its economy, so its cyber action is necessitated as costs preclude the sort of action that spanned the globe during the Cold War. Perhaps that will change. One never knows, but we may see them soon enough.