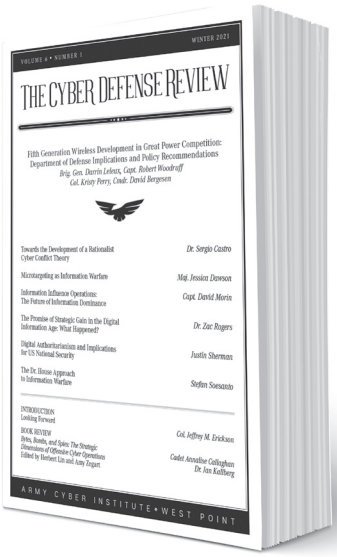
VOL. 6 ◆ NO. 1

The Cyber Defense Review: Looking Forward

Colonel Jeffrey M. Erickson



As 2020 was ending, there was a good deal of "Glad this year is over!" humor across social media. Of course, 2020 was unique with a global pandemic, but I think we all realize that the difference between the last day of 2020 and the first day of 2021 was not much more than a single rotation of the Earth. Most of the conditions between one moment to the next have not substantially changed.

However, one thing that is changing is an increasing awareness of the threat of cyber infiltration and attacks. Being a U.S. Presidential election year served as a focal point for cybersecurity, despite little evidence of disruption through electronic means. Instead, we learned of infiltration across vast amounts of industry and the United States Government (USG).

The SolarWinds attack highlighted the pervasiveness of threats across organizations and networks. With over 250-plus government agencies and businesses affected, it is becoming clear that no organization is safe.[1] Considering the reports that the intrusion occurred as early as March/April 2020, it highlights the challenges of maintaining and defending networks. Simply put, by the time you discover the threat, it is already too late. Instead, increasing situational awareness ahead of time becomes even more critical.

1 D. Sanger, N. Perlroth, and J. Barnes, "As Understanding of Russian Hacking Grows, So Does Alarm," *The New York Times*, accessed January 6, 2021, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html.

Colonel Jeffrey M. Erickson is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. As Director, COL Erickson leads a 60-person, multi-disciplinary research institute focused on expanding the Army's knowledge of the cyberspace domain. He began his Army career as an Armor officer before transitioning to the Simulation Operations functional area, where for the last 15 years, he has been using simulations to train from the individual to the Joint and Combatant Command levels. He has a B.S. in Computer Science from the United States Military Academy, an M.S. in Management Information Systems from Bowie State University, and an M.S. in National Resource Strategy from the Eisenhower School (formerly the Industrial College of the Armed Forces). His fields of interest are simulations for live-virtual-constructive training, testing, and wargaming.

To that end, *The Cyber Defense Review* Winter edition presents a great collection of authors from across the global community. We hope that these articles will expand your understanding of the challenges we face with respect to cyberspace while also providing recommendations on how to mitigate these issues.

With respect to new technologies, our Leadership Perspective article "Fifth Generation Wireless Development in Great Power Competition" by Brig Gen Darrin Leleux, CAPT Robert Woodruff, COL Kristy Perry, and CDR David Bergesen provide relevant thoughts and recommendations concerning the implementation of 5G technology. The authors identify the opportunities and risks associated with the 5G technologies by looking at the recommendations of the Defense Science Board, the Defense Innovation Board, and the European Commission. Through this analysis, the authors propose a potential whole-of-government approach in leading the implementation to mitigate security risks, both in and out of the USG.

In the area of Information Warfare/Operations, we have a diverse set of articles. The Army Cyber Institute's MAJ Jess Dawson provides a critical perspective on the increasing threat of micro-targeting and how the evolving surveillance economy poses a real threat to the mission readiness of military members and their families. She posits that this is becoming a potential force protection issue and will only increase unless the Department of Defense implements some mitigations. Dr. Zac Rogers (Flinders University, Australia) looks to fill the gap between information operations and cognitive warfare/security by looking to define the terms and their impact on warfare in his article "The Promise of Strategic Gain in the Digital Information Age: What Happened?" For a different perspective, Stefan Soesanto (ETH Zurich) provides a unique approach to Information Warfare, using the popular medical drama "House." Adopting the skeptical and blunt approach of Dr. House may counter

the frustratingly fast disinformation and misinformation campaigns of bad actors by focusing on their networks and not on their content. Finally, in our high-velocity Research Note section, CPT David Morin (93d Signal Brigade) proposes that the construct of Information Influence Operations (IIOs) will provide an approach to exert influence and strategic messaging within cyberspace.

At a strategic/state level, Dr. Sergio Castro (Instituto de Ciberdefensa, Mexico) proposes a model that correlates cyber operations and their broader strategic consequences in his article "Towards the Development of a Rationalist Cyber Conflict Theory." In "Digital Authoritarianism and Implications for US National Security," Justin Sherman (non-resident fellow at the Atlantic Council's Cyber Statecraft Initiative) highlights how the increasing use of technology by malicious state authorities can be used to entrench state power, increase domestic surveillance, and insulate regimes from external cyberattacks.

For those looking to expand their cyber library, United States Military Academy Cadet Annalise Callaghan and Dr. Kallberg from the ACI, provide a review of *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (ed. Herbert Lin and Amy Zegart). The anthology delivers some unique perspectives from a variety of authors on various facets of cyberspace.

As a reminder, our next issue will be a COVID-19 special edition (Spring 2021), capturing some thoughts on the pandemic's impact in the cyberspace environment, from our homes to our businesses to the highest levels of government.

Additionally, while the future of conferences remains uncertain, I encourage CDR readers to consider attending NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) Conference on Cyber Conflict (CyCon), occurring 25-28 May 2021 in Tallinn, Estonia. We hope to see you there (even virtually).

In conclusion, as we look forward to 2021, I like to use the term "skeptical optimism." This can best be defined as "seeing the glass as half full, but always brainstorming ways to fill the glass to the top."[2] Regardless of what 2021 brings, I am hopeful that the continuing dialogue of cyber professionals will continue to push the community to fill that glass.

2 L. Stevens, "On Being a Skeptical Optimist," accessed January 6, 2021, https://www.thinksplendid.com/blog/optimism-in-business.