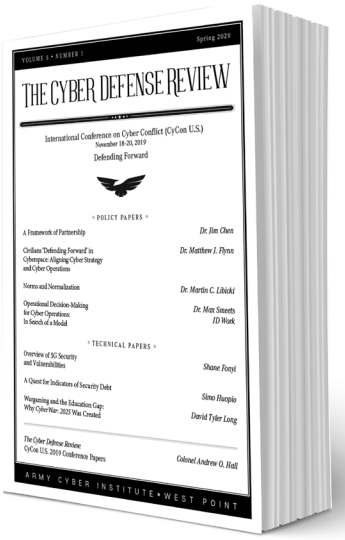
VOL. 5 ◆ NO. 1

The Cyber Defense Review: CyCon U.S. 2019 Conference Papers

Colonel Andrew O. Hall
Director, Army Cyber Institute
United States Military Academy



INTRODUCTION

Welcome to the Spring edition of *The Cyber Defense Review* (CDR), and the exciting publication of the CyCon U.S. 2019 conference papers. This edition of the CDR will feature 6 policy and 5 technical papers that dramatically provide texture and insight into the complicated Defending Forward strategy. The 11 papers were presented on November 18-20, at the Crystal Gateway Marriott in Alexandria, VA. The CyCon U.S. conference is the premier forum on cyber conflict. It is a collaborative effort between the Army Cyber Institute (ACI) at West Point and the NATO Cooperative Cyber Defence Centre of Excellence and complements the CyCon Conference held every spring in Estonia.

The CyCon U.S. conference theme was Defending Forward and followed the Department of Defense's (DoD) 2018 Cyber Strategy, which identified the need for active preparedness in cyberspace by "defending forward." This strategy intends to disrupt or halt malicious cyber activity at its source, and degrade said activity before it can reach its intended victim. The "defending forward" strategy engages the private sector as a pivotal ally in defending the nation's networks.

The 2019 conference was an immense success that was attended by 337 people from over 40 companies, 13 universities, 17 foreign nations, congressional staffers, and various government organizations. A post-event survey found that 92% of respondents reported the topics as being useful to their work, 93% thought that the event advanced the cyber body of knowledge, and 100% believed that it succeeded in creating or maintaining productive partnerships. Videos of the panels and speakers are posted on the ACI's website to allow a wider audience to access this valuable information: https://cyber.army.mil/. We thank all those who submitted papers, attended the conference, and worked so diligently behind the scenes to make this a spectacular event.

Colonel Andrew O. Hall is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. In his position as Director, Colonel Hall leads a 70-person, multi-disciplinary research institute and serves as the Chairman of the Editorial Board for *The Cyber Defense Review* (CDR) journal; and Conference Co-Chair for the International Conference on Cyber Conflict U.S. (CyCon U.S.). He has a B.S. in Computer Science from the USMA, an M.S. in Applied Mathematics from the Naval Postgraduate School, and a Ph.D. in Management Science from the University of Maryland. Colonel Hall additionally teaches in the Department of Mathematical Sciences and the Department of Electrical Engineering and Computer Science at the USMA. Since 1997, Colonel Hall's military career has been focused on operations research and solving the Army's most challenging problems using advanced analytic methods. Colonel Hall also serves as the President of the Military Applications Society of the Institute for Operations Research and the Management Sciences. His research interests include Military Operations Research, Cyber Education, Manpower Planning, and Mathematical Finance.

The CyCon U.S. conference committee selected 11 peer-reviewed scholarly papers for presentation at the conference from the 40 papers submitted for consideration (a 27% selection rate). These papers were presented at CyCon U.S. under the following two session topics: Policy and Technical. Following publication in the Spring CDR, the papers will be indexed in JSTOR for access by other cyber researchers.

The Spring CDR begins with the Policy papers and Dr. Jim Chen's "A Framework of Partnership Methods." He contends that cyberspace requires a partnership between the public and private sectors. Dr. Chen recommends a whole-of-society approach due to the holistic nature of cyber threats. The second article of the Spring CDR is Dr. Matthew Flynn's "Civilians 'Defending Forward' in Cyberspace: Aligning Cyber Strategy and Cyber Operation," which advocates for a new US military cyber strategy that relies on increased civilian involvement. In "Norms and Normalization," Dr. Martin Libicki brilliantly examines nation-state cyber activities and *de facto* norms in cyberspace. The fourth policy article is Alan Mears and Joe Mariani's "The Temporal Dimension of Defending Forward," which tackles U.S. Cyber Command policy from a UK perspective. Next up is "Defending Forward on the Korean Peninsula," by Dr. James Platte of the U.S. Air Force Center for Strategic Deterrence Studies (CSDS). He examines cyber deterrence in the Korean AOR as part of the overall strategic deterrence posture of the U.S.-ROK alliance. The Policy section ends with Dr. Max Smeets and JD Work's captivating study "Operational Decision-Making for Cyber Operations: In Search of a Model." Their work explores the complexity of cyber operations and the decision dynamics of cyber conflict.

Our CDR readers will thoroughly enjoy all five Technical papers. Shane Fonyi from the ACI crafts a superb and timely work that covers the 5G security space, technologies, and vulnerabilities in "Overview of 5G

Security and Vulnerabilities." Seth T. Hamman, Jelena Vićić, Jack Mewhirter, Philip White, and Richard J. Harknett collaborate on "Deciphering Cyber Operations: The Use of Methods and Simulations for Studying Military Strategic Concepts in Cyberspace." They brilliantly describe a simulation framework to study the dynamics of cyber operations below the threshold of armed attack. Forrest Hare and William Diehl's, "Noisy Operations on the Silent Battlefield" provide examples of non-intrusive precision cyber weapons used in real-world operations. Simo Huopio from the Finnish Defence Research Agency examines Technical Debt (TD) and offers an innovative solution framework in "A Quest for Indicators of Security Debt." The last article in this Spring Edition is David Tyler Long's "The Cyberspace Operations Wargaming and Education Gap," which highlights the importance of wargaming to the development of sound cyber policy and doctrine.

The next CDR will be our first themed edition and will focus on Information Operations (IO). Daily, our competitors are leveraging IO to influence what we believe, while intending to sow distrust and impact how we behave. IO is now a joint warfighting function, and the US military is focused on preparing to compete in Information Warfare (IW) to win future conflicts. We are honored to showcase articles from LTG Stephen Fogarty, Lt Gen Timothy Haugh, BG (Ret.) Jeff Smith, Dr. Martin Libicki, Bryan Sparling, Tim Thomas, Dr. Herb Lin, Dr. Chris Paul, and Renny Gleeson. This thought-provoking themed edition will explore the differences between IO and IW, tackles the media's role in IO, and analyze our adversaries' IO strategy during competition, pre-crisis, and conflict.

Please check our Call for Papers announcement on the CDR website to submit articles on "Cyber Economics" for a themed Spring 2021 CDR: https://cyberdefensereview.army.mil/. This issue will explore cyber's impact on the US economy, the data behind cyber economics, the cyber risk management, the monetary value of cyber incidents, the economics of national cyber strategy, and leadership and business decision-making. We welcome a multidisciplinary and international examination of this vital topic. I encourage our readers to submit cyber economic research papers, commentaries, research notes, and book reviews on the CDR *ScholarOne* platform: https://mc04.manuscriptcentral.com/cyberdr.

I want to recognize the extraordinary talent and creativity of Michelle Marie Wallace, Sergio Analco, Gina Daschbach, and Courtney Gordon-Tennant for transforming this signature edition. Please enjoy these thoughtful papers, and may their relevance guide our continued cyber conversation together!