VOL. 5 ◆ NO. 3

The Cyber Defense Review: Expanding the Cyber Discussion

Colonel Jeffrey M. Erickson

VOLUME 5 • NUMBER 3 FALL 2020

THE CYBER DEFENSE REVIEW

To Defend Forward, US Cyber Strategy Demands a Cohesive Vision for Information Operations
The Honorable Patrick Murphy
Dr. Erica Borghard

A Legal Framework Enhancing Cybersecurity through Public-Private Partnership
The Honorable Joe R. Reeder
Professor Robert E. Barnsby

Jack Voltaic®: Bolstering Critical Infrastructure Resilience
Maj. Gen. Robin L. Fontes
Maj. Erik Korn, Lt. Col. Doug Fletcher, Maj. Jason Hillman,
Lt. Col. Erica Mitchell, Maj. Steven Whitham

Cyber Maneuver and Schemes of Maneuver: Preliminary Concepts, Definitions, and Examples — *Dr. Patrick D. Allen*

Beyond Hyperbole: The Evolving Subdiscipline of Cyber Conflict Studies — *Dr. Aaron Brantly*

Why the Law of Armed Conflict (LOAC) Must be Expanded to Cover Vital Civilian Data — *Col. Beth Graboritz, Lt. Col. James Morford, Maj. Kelley Truax*

Implementing Intrusion Kill Chain Strategies by Creating Defensive Campaign Adversary Playbooks — *Rick Howard, Ryan Olson*

COVID-19: The Information Warfare Paradigm Shift — *Dr. Jan Kallberg, Dr. Rosemary A. Burk, Dr. Bhavani Thuraisingham*

INTRODUCTION
Expanding the Cyber Discussion — *Col. Jeffrey M. Erickson*

BOOK REVIEW
Cybercrime and Society
by Majid Yar and Kevin F. Steinmetz — *Stanley Mierzwa*

ARMY CYBER INSTITUTE ◆ WEST POINT

INTRODUCTION

Welcome to *The Cyber Defense Review* (CDR) Fall 2020 edition. As the new Director for the Army Cyber Institute (ACI), I am honored to be joining the CDR team and very excited about this most recent issue of the journal. The CDR plays a critical role in expanding the discussion within the cyber community, from tactical units to national leadership to industry partners to academia. The quality of articles from a diverse group of leaders and thinkers within the community, coupled with an extensive reach that includes foreign allies, partners, and international educational institutes, is a testament to the impact of this journal. The CDR is truly adding to the body of knowledge in the cyberspace domain.

Our Leadership Perspective portion provides unique perspectives with national impacts. Major General Robin Fontes (Deputy Command General (Operations), U.S. Army Cyber Command) and the ACI's Critical Infrastructure Team (Lieutenant Colonel Doug Fletcher, Lieutenant Colonel Erica Mitchell, Major Jason Hillman, Major Erik Korn, and Major Steven Whitham) address ways to increase the resiliency of public and private critical infrastructure through ACI's Jack Voltaic® project. Jack Voltaic®, which recently completed its third iteration involving the cities of Savannah, GA, and Charleston, SC, looked specifically at potential impacts on deploying forces as they utilize these key port cities.

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.

We are honored to showcase two articles that tackle key issues from the Cyberspace Solarium Commission. The Honorable Patrick Murphy (former Under Secretary of the Army) and ACI's Dr. Erica Borghard discuss how the United States should adopt a whole-of-nation, defend forward strategy for information operations. From a legal perspective, the Honorable Joe Reeder (former Under Secretary of the Army) and ACI's Professor Rob Barnsby posit that the Cyberspace Solarium Commission may have broken through the public-private partnership roadblocks with respect to performing cybersecurity by reinforcing the necessity of a collaborative approach. The recommendations in both articles have a potential national-level impact on how the US organizes for success in the cyberspace domain.

Rick Howard (Chief Analyst, Chief Security Officer, and Senior Fellow at The CyberWire) and Ryan Olson (Vice President of Threat Intelligence for Palo Alto Networks) provide a Professional Commentary on the value of developing adversary playbooks as a framework to enable cyber defense and intelligence sharing. I think you will find their proposed approach moving beyond Lockheed Martin's white paper on Cyber (Intrusion) Kill Chain, an interesting solution.

Within our Research Articles, authors address a variety of topics to include a proposed operational framework, a look at the tendency to describe the complex cyber-threat environment through exaggerated terms, a method to analyze the ever-growing Smart City environment, and a proposed change to the Law of Armed Conflict concerning civilian data. First, Dr. Patrick Allen (Information Operations Specialist at the Johns Hopkins University Applied Physics Laboratory) articulates both the need and an approach for describing cyber maneuvers at the operational level. His article not only provides categories of maneuver, but also applicable examples that any maneuver commander could use to integrate cyber domain operations with more conventional operations. Next, in "Beyond Hyperbole: The Evolving Subdiscipline of Cyber Conflict Studies," Dr. Aaron Brantley (Assistant Professor of Political Science at Virginia Tech and former Army Cyber Institute member) looks at scholarly works and argues for the need to move cyber conflict studies into the broader discipline of International Relations by shifting the discussion away from apocalyptic hyperbole to a focus on concrete, real-world examples.

Urban warfare has been a constant challenge for military forces. Considering the proliferation of Smart Cities, the increasing likelihood of future conflicts in these environments requires an understanding of the technologies and trends affecting the environment. Maxim Kovalsky (Senior Manager, Deloitte's Cyber Risk Advisory), Lieutenant Colonel Robert Ross (formerly ACI's Information Warfare Team Lead), and Greg Lindsay (non-resident fellow of the Atlantic Council) discuss the key trends in Smart Cities and propose a method for analyzing the ecosystems to inform intelligence preparation of the battlefield and enable military operations. Finally, the necessity to reclassify civilian data as an "object" is discussed in "Why the Laws of Armed Conflict Must Be Expanded to Cover Vital Civilian Data" by Colonel Beth Graboritz (Deputy Director, National Security Agency's Command, Control, Communications and Cyber Systems Directorate), Lieutenant Colonel James Morford (Deputy Director for Communications and Information at 7th Air Force), and Major Kelly Truax (Deputy Chief, Strategy and Policy Analysis Division, U.S. Transportation Command). This proposal would provide Laws of Armed Conflict protections for civilian data and allow for legal actions in response.

In the Research Notes section, First Lieutenant Hugh Harsono (Assistant Operations Officer in a Special Operations Task Force) discusses the challenges of digital threat financing, and the potential role Special Operations Forces could play in countering this growing challenge. Additionally, to address the current pandemic, Dr. Jan Kallberg, Dr. Rosemary Burk, and Dr. Bhavani Thuraisingham touch on some of the unknown second and third-order effects of the virus in "COVID-19: The Information Warfare Paradigm Shift." Looking ahead, we are accepting papers for a CDR COVID-19 themed issue in Spring 2021 related to the pandemic and the challenges related to cyberspace concerning security, technology, and policy. If you are interested in submitting a relevant article, please visit the CDR website for additional information: https://cyberdefensereview.army.mil/.

Finally, I would like to take a moment to recognize the departure of one of the ACI's team members, Dr. Erica Borghard. In her time with ACI, the impact of Erica's work has reached from the classroom to the halls of Congress. In addition to instructing at West Point, she served as a task force lead for the Cyberspace Solarium Commission, where she provided recommendations to the Nation's leadership on national policy and law related to cyberspace. She is departing to accept a position at the Atlantic Council, where she will continue to be a thought leader in the cyberspace realm. Good luck, Erica!

In conclusion, I am very honored to join *The Cyber Defense Review* team and excited about continuing the important dialogue with this august community. Let's move forward together!