VOL. 6 ◆ NO. 3

The Cyber Defense Review: Ransomware's Growing Impact

Colonel Jeffrey M. Erickson

Welcome to the Summer 2021 edition of *The Cyber Defense Review* (CDR) where you will find a collection of thought-provoking articles in this issue.

First, let us start with the elephant in the room: Ransomware. Ransomware has become a household name over the last year, with the frequency and scale of the attacks increasing at an alarming rate. We hear almost weekly of a significant attack affecting multiple organizations, both as primary targets and as downstream collateral targets. The recent Colonial Pipeline shutdown and JBS's meat processing plant disruptions demonstrated in very real terms the potential impacts of cyberattacks on large portions of the American population. Clearly, the status quo is not working.

To address this issue, the Honorable Joe R. Reeder (former Under Secretary of the Army) and United States Military Academy (USMA) Cadet Tommy Hall assess the implications of the Colonial Pipeline event and provide seven key lessons that the Nation must address in their article: "Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack."

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.

While ransomware is receiving most of the media's attention, our authors are also looking at other concerning trends and potential vulnerabilities worth considering:

- **Supply Chain Vulnerabilities:** Captain Kyle Sullivan asks the very pertinent question: Is the Mission Partner Environment (MPE) at risk due to equipment manufactured by possible adversaries? If you have concerns about NATO's ability to achieve the Federated Mission Network (FMN) and the United States' initiative to support it, you will find the article, "Risks to the Mission Partner Environment: Adversarial Access to Host Nation Network Infrastructure," riveting.
- **Russian Information Warfare:** Tobias Redington's article "RT and the Element of Disguise: Russia's Information Weapon," highlights RT's tactics and techniques to build legitimacy while practicing deception and mis/disinformation. He highlights examples of the dishonest behavior and mis-directions of this organization and its success in simultaneously building a global audience. His article is a call to action for Western governments and provides some possible options.
- **China's Approach to the Arctic:** The Arctic is continuing to become a focus for future defense-related issues. In his article, "China Arctic Cyber Espionage," Emilio Iasiello assesses China's approach to the region, through investment, mineral rights, and cyber espionage. Could this be setting the stage for a "Polar Silk Road?"

Additionally, many of our authors propose new approaches to build capability, see ourselves, and approach complex problems:

- **Unconventional Warfare:** In the article, "Technology Adoption in Unconventional Warfare," Sean Pascoli and Dr. Mark Grzegorzewski propose using the model of irregular and non-traditional forces

with cyber capabilities. Using methods such as employing cyber-capable irregular forces and cyber-proxies to deny infrastructure and networks to adversaries while enabling access to allies. As they aptly point out: how do we change the risk aversion mindset that enables proxies to conduct kinetic operations, yet will not enable actions in the cyber domain? Using the Seven Phases of Unconventional Warfare, they describe some of the actions UW forces could employ to support larger operations and strategic objectives.

- **Game Theory:** Hiram Henderson recommends the use of game theory to enable the Joint planning process in his article "Cybered Competition, Cooperation, and Conflict in a Game of Imperfect Information." Drawing from the lessons learned from nuclear deterrence, he provides some thoughts and planning considerations for a cyber-based approach.
- **Enhancing PMESII:** In their article, "Combined Information Overlay for Situational Awareness in the Digital-Anthropological Terrain: Reclaiming 'Information' for the Warfighter," Dr. Zac Rogers and Dr. Emily Bienvenue provide a construct that combines the familiar PMESII-PT (political, military, economic, social, information, infrastructure, physical environment, and time) taxonomy with the lesser-known Digital Anthropological Terrain (DAT) construct in a structured manner to inform decision-makers, and subsequently translate intent into action.
- **Cataloging Threats:** In "Attack-Based Network Defense," Major William North proposes the adoption of a standardized and quantifiable methodology to catalog known and unknown threat techniques to allow for better training, testing, synchronization, and incident response.

For those interested in expanding their understanding of artificial intelligence and robotics with respect to warfare, USMA Cadet Dylan Taylor and ACI's Major Mark Lesak have provided a book review of Paul J. Springer's *Outsourcing War to Machines: The Military Robotics Revolution*. They highlight the use of examples from the history of warfare and the revolutions in military affairs as they relate to the future employment of these systems.

The CDR is fortunate to have the brilliant design team of Sergio Analco and Gina Daschbach and world-class editors in Michelle Wallace, Dr. Jeff Morris, Courtney Gordon-Tennant, and LTC Mark Visger supporting the journal. The West Point Class of '70 Assistant Editors: Hon. Joe R. Reeder, Dr. Bill Spracher, Chip Leonard, and Dr. Bill Lane enhance every CDR article with their thought leadership and scholarly engagement. Again, thanks for joining us for the Summer issue, and we look forward to continuing the discussion on these topics through active engagement in the wider cyber community.