VOL. 7 ◆ NO. 2

The Cyber Defense Review: So...Anything Interesting Going On?

Colonel Jeffrey M. Erickson

As I read through the Spring CDR, I found that the war in Ukraine was on my mind and that I analyzed the articles through that lens. During my reading of each article, I kept asking myself the following:

- How does this relate to the current and evolving situation in Ukraine?
- Is Ukraine validating many of our assumptions of modern, multi-domain operations?
- Or is it a return to more traditional/conventional warfare?
- Finally, how are other adversaries, such as China, leveraging the situation to their own benefit?

While not written with Ukraine in mind, I think you'll find many relevant articles in this issue that highlight the need for continued thought leadership in cyberspace, which plays a crucial role in current and future competition and conflicts.

In our Leadership Perspective section, Admiral (Ret.) Dennis Blair (former U.S. Director of National Intelligence) and William "Bud" Roth, Esq. (781st Military Intelligence Battalion, U.S. Army) argue for the expansion of the role of the private sector in cybersecurity. They highlight historical examples where private companies have assisted with law enforcement activities and describe a three-tiered licensing system that would increase collaboration with the government and overall defensive capabilities. Additionally, the Honorable Christopher Ford (former U.S. Assistant Secretary of State for International

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

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.

Security and Nonproliferation) in "Conceptualizing Cyberspace Security Diplomacy" provides a framework around the variables of information strength, partner trust, and operational consequence as a way to inform responses to threats. The graphical representation of his framework provides a visualization of potential outcomes.

We are excited to showcase two outstanding Professional Commentaries in the Spring CDR. In his article "America's Cyber Auxiliary: Building Capacity and Future Operators," Lieutenant Colonel (Retired) Jeff Fair (Vice President of Cybersecurity and Economic Development at the San Antonio Chamber of Commerce) argues for the creation of a cyber auxiliary corps like the Coast Guard Auxiliary Corps and the Civil Air Patrol. Both organizations were created during times of great change to create the necessary capacity to serve the nation while simultaneously inspiring new generations. Could we leverage a similar model for our current environment? While the article "AI, Super Intelligence, and the Myth of Control," Brian Mullins (CEO, Mind Foundry) highlights the myths surrounding data, super intelligence, the role of humans in decision-making, and the barriers to achieving organizational intelligence.

Our Research Articles cover a variety of topics:

- In "Information as Power," Dr. Milton Mueller (Georgia Institute of Technology's School of Public Policy) and Dr. Karl Grindal (GIT's School of Cybersecurity and Privacy) discuss the evolution of Information Operations within the US military, to include how it was implemented in the Cold War, Global War on Terror, and post-2016 election. They examine how the various services have approached information warfare and the possible friction points with the traditional US views on freedom of speech and the exchange of information.

- In "Explicit Bargains are Essential to Forming Desired Norms in Cyberspace," Major Wonny Kim (Innovation and Information Operations Officer, 75th Innovation Command, U.S. Army) discusses the need for the US to better establish norms in cyberspace with respect to China through explicit policy, but also through actions. Failure to clearly define either could potentially lead to escalatory actions by both sides.
- In "Timing Influence Efforts with Information Processing," Dr. Joshua McCarty (Purdue University Global) and Kaylee Laakso explain how information is sought and narratives are formed following crisis events. They present case studies that demonstrate the criticality of the first five days of information seeking and the eventual socialization of the information. By understanding the life-cycle of this process, it's possible to leverage the window of opportunity to enable positive outcomes.
- Major Neill Perry (U.S. Air Force Reserves Intelligence Officer) discusses the US approach to disinformation in "The Global Engagement Center's Response to the Coronavirus Infodemic." He explores what worked and provides recommendations for the future.

Finally, Major Mathieu Couillard (Signals Officer, Canadian Armed Forces) provides an excellent review of John Arquilla's *Bitskrieg: The New Challenge of Cyberwarfare.* Arquilla's book seeks to define the complex current environment and provides some policy recommendations worth considering.

As Ukraine dominates the headlines, the ideas, concepts, and positions contained in this issue go beyond the current conflict to help our understanding of the enormous challenges and greater possibilities within cyberspace.