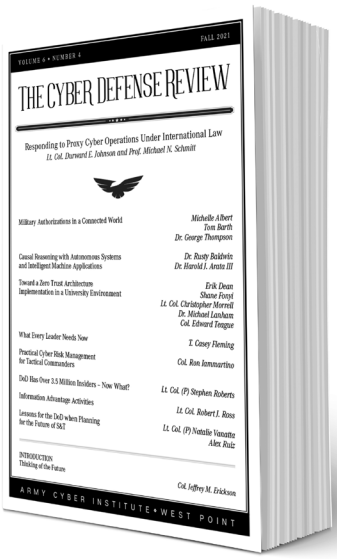
VOL. 6 ◆ NO. 4

The Cyber Defense Review: Thinking of the Future

Colonel Jeffrey M. Erickson



"It's tough to make predictions, especially about the future.""

–Yogi Berra (and many others...)

Since the publication of Johannes Kepler's novel, *Somnium*, science fiction has played an interesting role in society. It has been used to inspire (just ask how many current astronauts point to *Star Trek* as their reason for their chosen profession), to inform about possibilities (driverless cars have appeared in numerous films), or to serve as a warning (pick any post-apocalyptic movie...there's too many to list).

Many of the current cyberspace challenges we face were, at one time, the stuff of science fiction. While it is possible to fixate on the negative aspects of the current and future state, the many authors in this issue offer potential solutions for our challenges. Hopefully, their perspectives and proposals will move us beyond the status quo to reach a more advantageous state.

First, in the area of policy, our authors tackle the challenges of proxies and insider threats and propose solutions on where we need to go concerning these complex topics:

- **Cyber Proxies:** In "Responding to Proxy Cyber Operations under International Law," authors Michael Schmitt (Professor of International Law at the University of Reading in the United Kingdom) and U.S. Army Lieutenant Colonel Durward Johnson (Chief of Military Justice, III Corps and Fort Hood) discuss the challenges surrounding the use of proxies and the associated legalities and nuances concerning countermeasures. While there are current legal options, a more flexible interpretation and increasing

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.

use of these options will move DoD towards more effective deterrence.

- **Insider Threats:** Lieutenant Colonel Stephen Roberts (U.S. Army Cyber Command) poses an interesting question in "DoD Has Over 3.5 Million Insiders: Now What?" He identifies the risks (whether malicious or not) of having such a large number of individuals that may directly impact national security. He proposes a User Online Risk Score (UORS) model, similar to a FICO credit score, that measures a user's behaviors with respect to work to determine potential risks.

As technology continues to advance, DoD's approach to integration and implementation in future operations is critical, from the office to the battlefield.

- **Zero Trust Architecture (ZTA):** One of the evolving approaches to increase security in modern network environments is the Zero Trust Architecture. In "Toward a Zero Trust Architecture Implementation in a University Environment," the United States Military Academy (USMA) Information Technology team describes how West Point might implement zero trust principles to meet its mission as a premier academic institution while simultaneously serving as a U.S. Army organization.
- **Risk Management:** In his article, "Practical Cyber Risk Management for Tactical Commanders," Colonel Ron Iammartino (Army War College Fellow at Princeton University) proposes six decision rules that commanders can employ to take advantage of available technologies, services, and maintenance processes. Not only does this approach improve cybersecurity risk management, but it enables greater capability and adaption to cyber threats.
- **Artificial Intelligence:** The challenges with developing artificial intelligence through causal analysis are addressed in the article "Causal Reasoning with Autonomous Systems and Intelligent Machine

Applications," by Dr. Rusty Baldwin (University of Dayton) and Dr. Harold Arata (AT&T). By applying causal analysis to the fields of computer science and engineering, they argue that the potential for AI could reach the objective of human-like reasoning.

In addition to the technical aspects of the future environment, we are becoming more aware of the impact of complex information environment on individuals, societies, and nation-states.

- **Cyber Influence Operations:** In their article, "Military Authorizations in a Connected World: DoD's Role in Cyber Influence Operations," Michelle Albert, Tom Barth, and Dr. George Thompson (all from the Institute for Defense Analysis), discuss the challenges of competing in the gray zone and potential solutions to this capability gap. If we cannot find a way to win the "battle of the narrative" in the competition space, we may lose before the conflict even begins. This can be overcome with a new whole-of-government approach that includes relooking at existing laws and authorities. Sadly, while putting this issue together, we learned of the passing of Dr. Thompson. We are most grateful for his contributions to this issue.
- **Strategic Agility:** In "What Every Leader Needs Now: In This Unprecedented Era of Global Competition," Casey Fleming (Chairman and CEO of BlackOps Partners Corporation) calls for a cultural change in the business world with respect to the post-pandemic world. By applying the concepts of wargames used by military organizations, such as questioning assumptions, identifying/mitigating risk, and analysis of potential/likely future environments, businesses can set the conditions to evolve in the competitive space.
- **Information Advantage:** In "Information Activities: A Concept for the Application of Capabilities and Operational Art during Multi-Domain Operations," former ACI member and current Strategic Initiatives Chief to the Commanding General, Army Cyber Command (ARCYBER), LTC Robert Ross, proposes definitions and constructs to simplify the understanding of information and its relationship with future doctrine, information advantage, and the Army Warfighting Functions.
- **Forecasting the Long-Term Future:** In "Lessons for the DoD when Planning for the Future of S&T," ACI's Lieutenant Colonel Natalie Vanatta and advisor to the DoD, Alex Ruiz, describe the process they employed to inform the Office of the Under-Secretary of Defense (Research & Engineering)'s Science & Technology Roadmap which helps define potential technologies out to 2045. They touch on many of the complex factors affecting the current and future environments that must be addressed or mitigated to move DoD forward.

I hope these articles help stimulate your thoughts on the current state of the cyberspace domain and inspire you to look at setting conditions for a preferred future. I look forward to seeing you there (once we figure out *Star Trek*'s teleportation tech)!