Reimagining the Future

Deborah S. Karagosian

VOLUME 9 • NUMBER 3

FALL 2024

THE CYBER DEFENSE REVIEW

The Need for a Cyber Smoke Screen:
A Tactical Action that Instantly Becomes Strategic
in an All-Domain Operation
Dr. Dan G. Cox

The Path to China's Intelligentized Warfare:
Converging on the Metaverse Battlefield
Joshua Baughman

Blind Allegations of U.S. Cyber Hegemony
Complements China's Influence Campaign to
Weaken Global Confidence in the United States
Emilio Iasiello

GenAI in the 2024 Taiwan Presidential Election:
Lessons for Democracies
Maj. Sarah Mobilio

Embracing Memory Safe APIs for C2 Systems
Capt. Brian Yarbrough and Maj. Phelan Guan

Forward Persistence in Great Power Cyber Competition:
Military Assets in a Relative Power Erosion Framework
Dr. Thomas F. Lynch III

INTRODUCTION
Reimagining the Future

Editor-in-Chief,
Deborah S. Karagosian

ARMY CYBER INSTITUTE • WEST POINT PRESS

The Fall Edition of *The Cyber Defense Review* is largely influenced by the need for all of us to reimagine the future. How do we help create positions of relative advantage in competition while also preparing for future crisis and conflict? Our nation has recognized that the People's Republic of China (PRC) has studied how we conduct war and implemented approaches that, according to GEN Mark Milley, "pursue their strategic objectives while avoiding the deterrent tripwires upon which our national security posture is based." While we are "at war" in the cyber domain every day, the reality is we are a huge player in strategic competition. Reimagining the future includes making adjustments and preparing for crisis and conflict. As we study our adversaries and embark on new missions, technology continues to evolve, as do the ways people employ it.

Deborah S. Karagosian is the Editor-in-Chief of *The Cyber Defense Review* (CDR) at the United States Military Academy (USMA) at West Point, New York. In this capacity, she publishes the flagship cyber journal for the U.S. Army and Department of Defense. Before this assignment, she was an executive at two defense firms, entrepreneur, developer, consultant, and Soldier. She served the Army for 22 years with deployments to Asia, the Balkans, Africa, and the Middle East. She is a 1994 graduate of USMA and earned a M.S. in Computer Systems Engineering, an MBA in Strategic Management, and an MMAS from the School of Advanced Military Studies (SAMS).

Our cyber community is reimagining the future of warfare based on the lessons we learned, and continue to learn, in Nagorno-Karabakh, Gaza, Ukraine, and Israel. For good and bad, the innovative development of new technologies, applied in new ways in this battlespace will make it more lethal, reduce the ability to hide, and increase the tempo of war. The articles in this edition focus on visualizing the future operational environment, understanding our pacing threat, and leveraging lessons learned and research to improve our ability to compete and win.

This Fall Edition starts with Dr. Dan Cox of the School of Advanced Military Studies (SAMS) discussing "The Need for a Cyber Smoke Screen: A Tactical Action that Instantly Becomes Strategic in an All-Domain Operation." The proliferation of sensors across the battlefield is making our battle space increasingly transparent, necessitating cyber smoke screens to disable all sensors and devices in a region to successfully maneuver. While defensive in nature, a cyber smoke screen is an offensive cyber operation, suggesting that it may be time to integrate offensive and defensive cyber operations. Dr. Cox advocates for a cautious and mindful approach when military necessity calls for large-scale and prolonged disruption of internet services.

The intelligence community and our cyber mission forces will need a focused, sustained effort to understand the ever-changing terrain, both real-world and virtual, on and through which our Army will fight in the future. Preparing for information advantages will also require an understanding of the indigenous networks, peoples, and platforms where our Joint Force may be expected to compete or fight in the future. This edition contains three articles focused on understanding our pacing threat.

In his article, "The Path to China's Intelligentized Warfare: Converging on the Metaverse," Josh Baughman offers a unique perspective on how the PRC and the

People's Liberation Army (PLA) are leveraging emerging technologies in a new "intelligentized" era to create asymmetric advantages. In the PLA's "Meta-War," whoever can effectively integrate and connect the real world with virtual ones will have the "innovation high ground" to achieve the PRC's digital grand strategy and win future wars. His analysis provides timely and relevant insight into not only how the PLA thinks metaverse wars will be fought but also on how they envision they will be won.

The PRC strategically uses information to paint negative perceptions of U.S. actions within China and on the global stage. Everything in unclassified spaces, on the news, and in social media can be used by the Chinese Communist Party (CCP) to influence both their domestic population and international sentiment away from the U.S. and toward PRC goals. In "Blind Allegations of U.S. Cyber Hegemony Complements China's Influence Campaign to Weaken Global Confidence in the United States," Emilio Iasiello presents the cyber and geopolitical themes used by the PRC in Chinese and international news outlets and social media to label U.S. cyber activities as hegemonic, designed to exert influence and control the global internet, and to depict the U.S. as a "flawed democracy" that pervasively interferes in other state's affairs. Mr. Iasiello argues that PRC media campaigns may be aimed at influencing members of the United Nations to align with either a PRC or Russian preference for a government-led approach to internet governance to build "true power" by setting the standards and norms in the domain where such battles will be fought.

In his book *Next War: Reimagining How We Fight*, John Antal states artificial intelligence will change the speed at which we conduct war. But, if the PRC looks to achieve its national digital strategy without combat, how will it use technology during competition, and how can we counter it without raising the stakes? Major Sarah Mobilio discusses how the PRC used GenAI to influence Taiwan's 2024 national election and how the government of Taiwan responded in "GenAI in the 2024 Taiwan Presidential Election: Lessons for Democracies." While the PRC has increasingly used GenAI to craft subtle and increasingly undetectable influence campaigns, Taiwan's multi-faceted response, which included legislative actions, media literacy initiatives, and the development of its own GenAI tools, offers valuable insights for other countries facing similar challenges. Reimagining the future may include developing AI to counter the AI being used against us.

As our Army and Joint Force seek to gain positions of relative advantage in the information space, Captain Brian Yarbrough and Major Phelan Guan discuss the urgent need for "Embracing Memory-Safe APIs for C2 Systems." The information exchange enabled by Joint All-Domain Command and Control (JADC2) and many innovative initiatives throughout the force rely on the secure implementation of Application Program Interfaces (APIs). However, using inherently insecure languages creates strategic and tactical risks to DoD command and control, artificial intelligence, and legacy systems. Captain Yarbrough and Major Guan present these risks while providing recommendations for migrating to modern memory- and type-safe programming languages and mitigating risks from other languages. We need to re-imagine software development for our DoD systems and all public and private sector systems that rely extensively on APIs to communicate between systems and conduct business logic.

Similar to the risks Captain Yarbough and Major Guan address above, adversary targeting of a vulnerability is not limited to DoD networks. Attacks on critical national infrastructure are becoming a new normal in U.S. society. This era of Great Power Competition has led to changes in U.S. national strategies, and within DoD we are reimagining how to fight along the continuum of military operations. Dr. Tom Lynch of the National Defense University proposes the U.S. pursue a Relative Power Erosion framework that uses all elements of U.S. national power to create strategic cyber campaigns (and counter cyber campaigns) designed against PRC and Russian cyber organizations. He states that while USCYBERCOM's persistent engagement and hunt forward strategy appears effective in the near term, it is not sufficient for the longer term. Dr. Lynch suggests that the U.S. establish civilian interagency teams to operate as the military CMF teams operate today as they would be better suited to a whole-of-government approach for creating relative power gains and countering the efforts of U.S.'s great power rivals.

The technology and innovation inherent in our profession require the members of our community to learn constantly. We are always looking at vulnerabilities, the TTPs of hackers, and ways to employ new technologies to make our domain more secure and create new ways to access and impose our will on and through the networks of our adversaries. Reimagining the future requires our community to expand our thinking to understand more of the world around us and how our great power rivals are leveraging information, the electromagnetic spectrum, and cyberspace to build power. We hope the articles presented here increase your knowledge, expand your understanding, and make you think about how to compete and win in the future. We look forward to you sharing your thoughts and research with us.

—DSK

DISCLAIMER

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the U.S. Government.