VOL. 5 ◆ NO. 2

The Cyber Defense Review: Summer Special Edition on IO/IW

Colonel Andrew O. Hall
Lieutenant Colonel Robert J. Ross

INTRODUCTION

Welcome to our first themed edition of *The Cyber Defense Review* (CDR). Our inaugural themed edition is focused on information operations (IO) and information warfare (IW). IO and IW are not new constructs within the history of conflict. However, the exponential adoption and weaponization of social media technologies are rapidly changing the character of modern conflict. Soon digitally networked technologies known as the Internet of Things (IoT) will widely come online and supercharge the precision and reach of social media to enable unprecedented influence of targeted populations. These powerful information technologies are enabling our adversaries to achieve strategic goals and objectives that avoid our military strengths within the spaces short of armed conflict. As evidenced in 21st century conflicts thus far, the ubiquitous and amplifying effects of Information Age technologies are being used by our adversaries in ways that create a symphony of chaos, confusion, and polarization of targeted populations. These capabilities provide militarily inferior adversaries with the ability to achieve information parity at the minimum and information advantage at the maximum. If left unchecked, access to inexpensive and increasingly powerful commercial off-the-shelf (COTS) technologies will continue to provide our adversaries with the means to achieve information advantage in continuously innovative ways at a fraction of the cost of conventional warfare. The continual advancement of powerful information technologies is being used to create information weapons with devastating cognitive effects that pose an existential threat to the world order while leaving attribution for their deployment increasingly difficult. Developing the military's information advantage presents enormous legal and moral challenges in the areas of data privacy, artificial intelligence (AI), and across the social media platforms that our

Colonel Andrew O. Hall is the Director of the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. In his position as Director, Colonel Hall leads a 70-person, multi-disciplinary research institute and serves as the Chairman of the Editorial Board for The Cyber Defense Review (CDR) journal; and Conference Co-Chair for the International Conference on Cyber Conflict U.S. (CyCon U.S.). He has a B.S. in Computer Science from the USMA, an M.S. in Applied Mathematics from the Naval Postgraduate School, and a Ph.D. in Management Science from the University of Maryland. Colonel Hall additionally teaches in the Department of Mathematical Sciences and the Department of Electrical Engineering and Computer Science at the USMA. Since 1997, Colonel Hall's military career has been focused on operations research and solving the Army's most challenging problems using advanced analytic methods. Colonel Hall also serves as the President of the Military Applications Society of the Institute for Operations Research and the Management Sciences. His research interests include Military Operations Research, Cyber Education, Manpower Planning, and Mathematical Finance.

global competitors leverage. The changing character of information use in 21st century warfare has led the Department of Defense (DoD) to transform our military into a force capable of achieving information advantage and success during competitive and conflict operations in the information environment (OIE).

In 2018, the U.S. Army Cyber (ARCYBER) Commander, LTG Stephen Fogarty, committed to a strategy for transforming ARCYBER into an IW command by 2028. Several factors led to this decision: apparent Russian interference in the 2016 U.S. Presidential election; the convergence of the Army's IO, cyber operations, and electronic warfare (EW) capabilities within ARCYBER; and the Army's new multi-domain operations (MDO) concept. The complexities of this task are anything but trivial. The Army Cyber Institute (ACI) leadership recognized the need to support this endeavor and, in early 2019, created an IW team to support ARCYBER's transformational efforts. Since the IW team's inception, we have been dedicated to expanding the Army's and the nation's body of knowledge regarding how to organize, strategize, and integrate technology for success in future multi-domain operations. The IW team successfully established effective relationships with information professionals across academia, industry, and DoD. During this same time, our IW team hosted conferences, workshops, and collaborative meetings that connected some of the nation's foremost information technology, cyber, and advertising expertise with Army leaders. Together, we developed the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) for the creation of a powerful Information Age force.

The ACI IW team's deep and meaningful relations have led to the powerful partnerships and collaborations reflected by the world-class contributors to this "IO and IW Special Edition." The CDR and the ACI's IW team are honored to open this inaugural themed

Lieutenant Colonel Robert J. Ross is the Information Warfare Team Lead in the Army Cyber Institute at the United States Military Academy (USMA) located at West Point, New York. Lieutenant Colonel Ross leads a 7-person, multidisciplinary research team dedicated to expanding the Army's and the nation's body of knowledge on cyber and Information Age conflict. He has a B.S. in Computer Science from Rowan University, an M.S. in Computer Science from Monmouth University, and a Ph.D. in Information Science from the Naval Postgraduate School. Additionally, Lieutenant Colonel Ross is an assistant professor in the Electrical Engineering and Computer Science Department at USMA, who primarily teaches information technology courses. Lieutenant Colonel Ross is currently a cyberwarfare officer and former artilleryman with two combat deployments to Iraq. His research interests are organizational science, strategic foresight, information warfare education, and digital economics.

edition of the CDR with senior leader perspectives from LTG Stephen Fogarty (ARCYBER Commander), Lt Gen Timothy Haugh (16th AF Commander), and COL Michael Jackson (former EUCOM J39). Our opening senior leader article titled "Enabling the Army in an Era of Information Warfare," is co-authored by LTG Fogarty and COL (Ret) Bryan Sparling. This article articulates ARCYBER's strategy for the transformation from a command primarily focused on cyber electromagnetic activities to an expanded role that enables the Army to operate effectively in the information environment. Lt Gen Haugh, Lt Col Nicholas Hall, and Maj Eugene Fan co-authored the second article titled "Information Warfare Convergence." The article outlines the Air Force's unifying approach of convergence to synchronize daily Cyberspace; Intelligence, Surveillance, and Reconnaissance (ISR); Electromagnetic Warfare (EW); IO; IW; and Weather operations across the conflict continuum to support the joint force's ability to compete, deter, and win wars across all domains. The final article in our senior leader perspective's section is contributed by COL Jackson and Dr. Paul Lieber and is titled "Countering Disinformation: Are We Our Own Worst Enemy?," which provides interagency solutions for confronting state-sponsored disinformation.

Our professional commentary section features two exciting articles focused on the technical, cognitive, and strategic dimensions of contemporary information environments. The first article is written by MAJ Nathaniel Bastian and is titled "Building the Army's AI Workforce." Our second professional commentary piece is authored by Mr. Renny Gleeson, Managing Director of the Big Innovation Group at Wieden+Kennedy, titled "Truth Dies First: Storyweapons on the InfoOps Battlefield." In this article, Mr. Gleeson uses his unique insight acquired from a long history in the advertising industry to describe Storyweapons as a new class of threat, fielded by new threat actors in non-traditional domains across the digital landscape.

The CDR is honored to showcase four of the nation's leading academics in the field of information warfare and cyber defense in our Research section. The first article in this section, "Cyberwar is What States Make of It," by Dr. Martin Libicki discusses the ability of the attacker and recipients of cyber-attacks alike, to downplay or exaggerate the effects of these attacks based on the strategic objectives and consequences of the involved nation-states. Our second research article, "Doctrinal Confusion and Cultural Dysfunction in DoD: Regarding Information Operations, Cyber Operations, and Related Concepts," by Dr. Herb Lin presents an insightful examination of the tangled and confused history of information operations, cyber operations, and psychological operations doctrine in DoD. Our third research article, "Understanding and Pursuing Information Advantage," by Dr. Christopher Paul, is a masterful study that unpacks and explores the information advantage concept and how the U.S. Army and the joint force should consider it more broadly. Timothy Thomas wrote the final contribution to the IO and IW Special Edition of the CDR, "Information Weapons: Russia's Nonnuclear Strategic Weapons of Choice." He provides a very logical explanation for the Russian information weapons concept and its applications in 21st century warfare.

This fall, we are excited to present a non-themed edition that will feature a formidable group of leaders and scholars. The CDR will showcase the work of MG Robin Fontes, the Hon. Joseph Reeder, the Hon. Patrick Murphy, Dr. Patrick Allen, Prof. Robert Barnsby, Dr. Erica Borghard, Dr. Aaron Brantly, Dr. Sergio Castro, Dr. Jan Kallberg, and Maj Kelley Truax. This thought-provoking issue will be released in November.

The CDR seeks research papers, commentaries, and research notes related to cyber and the COVID-19 pandemic. This special edition will be published as the Spring 2021 CDR, and will explore "COVID-19 Implications for Cyber" in the context of (1) Data Privacy and Surveillance, (2) Exploitation of Fear, Anxiety, and Social Upheaval, (3) Preparedness and Resilience, (4) National Security Implications, and (5) Sources of Information and Disinformation. Please check our Call for Papers announcement on the CDR website. We welcome a multidisciplinary and international examination of this critically important topic.

We want to personally thank and recognize the remarkable dedication, energy, talent, and creativity of Michelle Marie Wallace, Sergio Analco, Gina Daschbach, SGM Jeff Morris, and Courtney Gordon-Tennant. The members of the West Point Class of '70: Joe Reeder, Bill Spracher, Chip Leonard, and Bill Lane, provided exceptional editorial support in the shaping and influencing of this special edition of the CDR. As always, we are excited to continue the cyber conversation together!