

# THE CYBER DEFENSE REVIEW

---

\*\*\*

Special Edition: Information Operations/Information Warfare



Enabling the Army in an Era of Information Warfare

*Lieutenant General Stephen G. Fogarty*

*Colonel (Ret.) Bryan N. Sparling*



16<sup>th</sup> Air Force and Convergence for the Information War

*Lieutenant General Timothy D. Haugh*

*Lieutenant Colonel Nicholas J. Hall*

*Major Eugene H. Fan*



Truth Dies First: Storyweapons  
on the InfoOps Battlefield

*Renny Gleeson*

Countering Disinformation:  
Are We Our Own Worst Enemy?

*Colonel Michael J. Jackson*  
*Dr. Paul Lieber*

Cyberwar is What States Make of It

*Dr. Martin Libicki*

Doctrinal Confusion and Cultural  
Dysfunction in DoD

*Dr. Herb Lin*

Understanding and Pursuing Information Advantage

*Dr. Christopher Paul*

Information Weapons: Russia's  
Nonnuclear Strategic Weapons of Choice

*Timothy Thomas*

---

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

*Colonel Andrew O. Hall*  
*Lieutenant Colonel Robert J. Ross*



# THE CYBER DEFENSE REVIEW

◆ SUMMER EDITION ◆



# THE CYBER DEFENSE REVIEW

## A DYNAMIC MULTIDISCIPLINARY DIALOGUE

### EDITOR IN CHIEF

Dr. Corvin J. Connolly

### MANAGING EDITOR

Dr. Jan Kallberg

### ASSISTANT EDITORS

West Point Class of '70

### AREA EDITORS

Dr. Harold J. Arata III  
(Cybersecurity Strategy)

Prof. Robert Barnsby, J.D.  
(Cyber & International Humanitarian Law)

Maj. Nathaniel D. Bastian, Ph.D.  
(History/Intelligence Community)

Dr. Aaron F. Brantly  
(Policy Analysis/International Relations)

Dr. Dawn Dunkerley Goss  
(Cybersecurity Optimization/Operationalization)

Dr. David Gioe  
(History/Intelligence Community)

Col. Paul Goethals, Ph.D.  
(Operations Research/Military Strategy)

Dr. Michael Grimaila  
(Systems Engineering/Information Assurance)

Dr. Steve Henderson  
(Data Mining/Machine Learning)

Ms. Elsa Kania  
(Indo-Pacific Security/Emerging Technologies)

Maj. Charlie Lewis  
(Military Operations/Training/Doctrine)

Dr. Fernando Maymi  
(Cyber Curricula/Autonomous Platforms)

Lt. Col. Erica Mitchell, Ph.D.  
(Human Factors)

Lt. Col. William Clay Moody, Ph.D.  
(Software Development)

Sgt. Maj. Jeffrey Morris, Ph.D.  
(Quantum Information/Talent Management)

Ms. Elizabeth Oren  
(Cultural Studies)

Dr. David Raymond  
(Network Security)

Dr. Paulo Shakarian  
(Social Threat Intelligence/Cyber Modeling)

Dr. David Thomson  
(Cryptographic Processes/Information Theory)

Dr. Robert Thomson  
(Learning Algorithms/Computational Modeling)

Lt. Col. Mark Visger, J.D.  
(Cyber Law)

### EDITORIAL BOARD

Col. Andrew O. Hall, Ph.D. (Chair.)  
U.S. Military Academy

Dr. Amy Apon  
Clemson University

Dr. Chris Arney  
U.S. Military Academy

Dr. David Brumley  
Carnegie Mellon University

Dr. Martin Libicki  
U.S. Naval Academy

Ms. Merle Maigre  
CybExer Technologies

Dr. Michele L. Malvesti  
Financial Integrity Network

Dr. Milton Mueller  
Georgia Tech School of Public Policy

Dr. Hy S. Rothstein  
Naval Postgraduate School

Dr. Bhavani Thuraisingham  
The University of Texas at Dallas

Ms. Liis Vihul  
Cyber Law International

Prof. Tim Watson  
University of Warwick, UK

### CREATIVE DIRECTORS

Sergio Analco  
Gina Daschbach

### LEGAL REVIEW

Courtney Gordon-Tennant, Esq.

### PUBLIC AFFAIRS OFFICER

Capt. Lisa Beum

### KEY CONTRIBUTORS

Clare Blackmon  
Nataliya Brantly

Kate Brown  
Erik Dean

Martha Espinoza  
Col. Michael Jackson

Lance Latimer  
Eric Luke

Alfred Pacenza  
Diane Peluso

Michelle Marie Wallace

### CONTACT

Army Cyber Institute  
Spellman Hall  
2101 New South Post Road  
West Point, New York 10996

### SUBMISSIONS

The Cyber Defense Review  
welcomes submissions at  
[mc04.manuscriptcentral.com/cyberdr](http://mc04.manuscriptcentral.com/cyberdr)

### WEBSITE

[cyberdefensereview.army.mil](http://cyberdefensereview.army.mil)

The Cyber Defense Review (ISSN 2474-2120) is published by the Army Cyber Institute at West Point. The views expressed in the journal are those of the authors and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government. The mention of companies and/or products is for demonstrative purposes only and does not constitute endorsement by United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

© U.S. copyright protection is not available for works of the United States Government. However, the authors of specific content published in The Cyber Defense Review retain copyright to their individual works, so long as those works were not written by United States Government personnel (military or civilian) as part of their official duties. Publication in a government journal does not authorize the use or appropriation of copyright-protected material without the owner's consent.

This publication of the CDR was designed and produced by Gina Daschbach Marketing, LLC, under the management of FedWriters.

The CDR is printed by McDonald & Eudy Printers, Inc. ∞ Printed on Acid Free paper.

## INTRODUCTION

**COLONEL ANDREW O. HALL**  
**LIEUTENANT COLONEL ROBERT J. ROSS**

9

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

---

## SENIOR LEADER PERSPECTIVE

**LIEUTENANT GENERAL STEPHEN G. FOGARTY**  
**COLONEL (RET.) BRYAN N. SPARLING**

17

Enabling the Army in an Era  
of Information Warfare

**LIEUTENANT GENERAL TIMOTHY D. HAUGH**  
**LIEUTENANT COLONEL NICHOLAS J. HALL**  
**MAJOR EUGENE H. FAN**

29

16<sup>th</sup> Air Force and Convergence  
for the Information War

**COLONEL MICHAEL J. JACKSON**  
**DR. PAUL LIEBER**

45

Countering Disinformation:  
Are We Our Own Worst Enemy?

---

## PROFESSIONAL COMMENTARY

**MAJOR NATHANIEL D. BASTIAN, PH.D.**

59

Building the Army's Artificial  
Intelligence Workforce

**RENNY GLEESON**

65

Truth Dies First: Storyweapons  
on the InfoOps Battlefield

---

## RESEARCH ARTICLES

**DR. MARTIN LIBICKI**

77

Cyberwar is What States Make of It

**DR. HERB LIN**

89

Doctrinal Confusion and  
Cultural Dysfunction in DoD

**DR. CHRISTOPHER PAUL**

109

Understanding and Pursuing  
Information Advantage

**TIMOTHY THOMAS**

125

Information Weapons: Russia's  
Nonnuclear Strategic Weapons of Choice

---





# THE CYBER DEFENSE REVIEW

◆ INTRODUCTION ◆



## *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) unprecedented influence of targeted populations will widely come online and supercharge the precision and reach of social media to enable 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 21<sup>st</sup> 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

*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 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 21<sup>st</sup> 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, education, personnel, facilities, and policy (DOTMLPF-P) for the creation of a powerful Information Age Force.

The 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. 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 21<sup>st</sup> 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! 







# THE CYBER DEFENSE REVIEW

◆ SENIOR LEADER PERSPECTIVE ◆



# Enabling the Army in an Era of Information Warfare

---

Lieutenant General Stephen G. Fogarty

Colonel (Ret.) Bryan N. Sparling

We cannot be an Industrial Age Army in the Information Age. We must transform all linear industrial age processes to be more effective, protect our resources, and make better decisions.<sup>[1]</sup>

*- General James C. McConville, 40<sup>th</sup> Chief of Staff of the U.S. Army*

Operations against ISIS, disrupting Russian attempts to interfere in the 2018 US midterm elections and, most recently, countering Iran's attempts to increase instability across the Middle East mark important efforts by the US military to find effective capabilities, doctrinal concepts, and appropriate roles in an era of information warfare. We must fight the battles our adversaries put before us. If our doctrines, systems, and processes do not match that reality, then it is time for new thinking. Through three decades of near-cessless global operations, "Information Operations," or IO has endured as the mainstay approach for how the Armed Services and the Joint Force conceptualize and apply informational power as an integral element of military operations. Despite evolving definitions, ever-changing formulations, and passionate assertions as to both its criticality and utility, IO remains doctrinal and relevant, though often misunderstood, a term of military art. Most often, IO has proved useful at tactical and operational levels of war. At more strategic and political levels, the efficacy of IO remains elusive, and US leaders, both civilian and military, have been less than adept at effectively realizing the potential of "informational power."

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



**Lieutenant General Stephen G. Fogarty** is the Commander, U.S. Army Cyber Command (ARCYBER). With more than 37 years of active service, LTG Fogarty was previously the first Commanding General of the U.S. Army Cyber Center of Excellence, and Commander, U.S. Army Intelligence and Security Command. His extensive Joint and Combined experience include assignments with U.S. Special Operations Command, U.S. Central Command, U.S. Cyber Command, three tours in Afghanistan, and Operation JUST CAUSE, Panama. LTG Fogarty holds Master's degrees in Administration from Central Michigan University and in Strategic Studies from the U.S. Army War College.

Given the US imperative of civilian control, and the military's supporting role in peacetime strategy and diplomacy, a perceived need for the military to play an expanded role, beyond tactical IO, in strategic, information-based influence remains limited and often contentious. The stunning social media-powered rise of ISIS in 2015, Russia's interference in the 2016 US Presidential election, Iran's increasing digital belligerence, and China's disinformation surrounding the COVID-19 pandemic are upending that perception and igniting a conversation across the defense establishment regarding appropriate roles for the uniformed armed services in this environment of unprecedented information warfare. Should the armed forces provide capabilities to protect not only US portions of cyberspace and the electric magnetic spectrum, but also the larger, and more challenging, Information Environment (IE)?<sup>[2]</sup> The Joint Chiefs of Staff have put forth the term "Operations in the IE (OIE)" to describe the Joint Force's growing informational mission; however, across the broader national security community, the term "information warfare (IW)"<sup>[3]</sup> is increasingly employed to connote an evolving suite of cyber, electromagnetic, and informational activities that the Army and other services are, or perhaps should be, developing, as part of a whole of government approach to counter adversary attempts to destabilize the US and its allies, and sustain a strategic competitive advantage in the IE.

The Army is currently evaluating whether OIE, IW, or some other concept should replace IO to describe an expanded Army mission in the IE. We are likewise considering whether Army Cyber Command (ARCYBER) should change its name to more accurately reflect the full spectrum of its mission portfolio. Regardless, ARCYBER is building upon a ten-year foundation of continual innovation, and accelerating its modernization efforts to enable information age Army operations across tactical, operational, and strategic echelons. As a functional Army Service Component Command (ASCC), ARCYBER



**Colonel (Ret.) Bryan N. Sparling** is a Highly Qualified Expert (HQE) serving as ARCYBER's Information Warfare Transformation Advisor. Sparling served over 27 years on active duty as a Signal Officer and Information Operations Officer. He was the Chief of IO and Special Activities, J39, U.S. European Command, 2011-2015, and the NATO Communication Director in Afghanistan, 2010-2011. He is a graduate of the U.S. Army School of Advanced Military Studies (SAMS), the National Defense University's Joint Advanced Warfighting School (JAWS), and holds a Masters in Telecommunications from the University of Colorado, Boulder.

supports Army and Joint Commanders by executing three major functions, detailed in Army Regulation (AR) 10-87<sup>[4]</sup>:

- 1. Conduct operations** – Commander ARCYBER is dual-hatted as Commander Joint Force Headquarters – Cyber (Army) and plans, integrates and executes full-spectrum Cyber Operations (operate, defend, attack), Electronic Warfare (EW) and IO missions in support of US Cyber Command (USCC), designated Geographic Combatant Commands, and the Army.
- 2. Provide forces** – ARCYBER supports USCC with Army Cyber Forces and supports Army operational commanders with tailored Cyber, IO, and EW forces. ARCYBER is the Title 10, “*Organize, Train, and Equip*” headquarters for specific force types identified by the Secretary of the Army.
- 3. Accelerate the state of Army information convergence** – ARCYBER is the central focal point for identifying, synchronizing, and advocating operational Cyber, IO, EW, and other information capability needs supporting Army and Joint operational missions.

Central to all these functions is the Army Network. As the foundational weapon system of a global, information age, land force, the Army Network is one of six specified Army modernization priorities.<sup>[5]</sup> Today, US forces are continually engaged in simultaneous competition and conflict around the world. Our adversaries recognize that our formations are highly dependent on data and connectivity, and thus our network presents a critical vulnerability. ARCYBER is the builder, operator, and defender of the Army sector of the Department of Defense (DoD) Information Network (DODIN-A). ARCYBER's ability to successfully defend the network, data, and interconnected weapons platforms from adversary attack is a critical prerequisite for all successful Army and Joint operations.

Within ARCYBER, and this article, “IW” refers to the converged employment of Cyber Operations (CO), EW, and IO forces, and the capabilities that support Army and Joint operations. Acknowledging the more extensive transformational requirements of the Army and the broader national security system, IW here refers to increasing the effectiveness of assigned ARCYBER forces through a mission-designed organization, experimentation, innovation, and systematic learning. By routinely deploying and employing converged IW formations, ARCYBER gains knowledge and experience through “sets and reps” as part of a larger Army campaign of learning.

## **THE ARCYBER TRANSFORMATION CAMPAIGN**

To fulfill the full spectrum of AR 10-87 responsibilities, both specified and implied, and anticipating emerging requirements driven by accelerating technology advances, ARCYBER has committed to a multi-year modernization effort. The ARCYBER transformation is envisioned to last more than ten years and is focused on supporting the Army’s evolving Multi-Domain Operations (MDO) concept. Through deliberate iteration, ARCYBER will play a critical role in the total Army’s capacity and skill to operate within and achieve operational advantage through the IE. Army actions, contributing to Joint OIE effects, will involve continuously posturing, and skillfully communicating (or obscuring), the location, capability, and intent of Army forces to influence the decision calculus and behavior of principal adversaries. This work involves the integrated employment of conventional land forces together with information and cyberspace capabilities, synchronized through as-yet-undeveloped combined information arms techniques. ARCYBER must enable the operational Army to sense, understand, decide, act, and assess more rapidly than our adversaries and enable Army and Joint Commanders’ ability to achieve decision advantage.

Internally, ARCYBER will work to build information capabilities into combined arms teams with converged cyber, influence, and electromagnetic capabilities that deploy to bring immediate, turn-key informational combat power to maneuver commanders. Externally, ARCYBER will work with TRADOC and the broader institutional Army to build IE literacy into commissioned and noncommissioned officer training and curricula, that we might collectively cultivate a new, 21<sup>st</sup> century Operational Art that leverages the ever-growing force of information and communication to amplify and empower the timeless, coercive power of violence. Simultaneous, parallel efforts—ARCYBER internal reorganization and transformation, external engagement and support to total Army information modernization efforts, and sustained experimentation and innovation in Army operations and execution of assigned Joint missions—will allow ARCYBER to provide a powerful center of gravity for improving land power effectiveness in modern military operations. Key to our success will be our ability to partner effectively with the U.S. Army Reserve and Army National Guard Cyber, and Information Forces.

The first phase of modernization, already well underway, aims to achieve irreversible momentum toward full-spectrum, integrated IW capability by the summer of 2021. From mid-2021 through 2028, Phase 2 will continue experimentation and innovation to meet operational

opportunities and challenges presented by emerging technologies. Sitting at a unique nexus of the operational and institutional sides of the Army, ARCYBER will connect academia, industry, and Army acquisitions directly to ongoing operations, and rapidly integrate cutting-edge solutions into the operational force. Beginning in 2028, Phase 3 will see the resourcing and fielding of IW capabilities and formations, tailored to enable IW in support of MDO. ARCYBER deployable capabilities will augment information capabilities by then increasingly organic to maneuver formations, that enable the Army to dominate competitive environments short of armed conflict, and set conditions for the Army to prevail, where deterrence fails.

ARCYBER's transformation will be significantly less successful without thoughtful integration of Army Reserve and Army National Guard Cyber, and Information Warfare capabilities and forces.

## **ARCYBER PROGRAMS AND INITIATIVES**

**Phase 1—by Mid-2021, Achieve Irreversible Momentum.** Multiple programs and new formations are already expanding ARCYBER's reach and effectiveness; these include:

- ◆ ARCYBER Headquarters move from Fort Belvoir, VA, to Fort Gordon, GA. In preparation for more than five years, 2020 will see this relocation of the ARCYBER Commander and headquarters staff to a state-of-the-art-facility co-located with the National Security Agency, and thereby optimizing seamless access to critical infrastructure enabling ARCYBER's core defense, offense, and network operations missions. For the first time, the Army's operational and institutional Cyber forces will enjoy unprecedented synergies by operating from a single, information power projection platform.
- ◆ Cyber Protection Brigade (CPB)—Activated at Fort Gordon in 2014, the CPB trains and deploys specialized Cyber Protection Teams (CPTs) to defend key cyberspace terrain. CPTs augment supported unit network defense ability to provide advanced assessments and defense against sophisticated and persistent cyber threats on Army and partner networks, systems, and data within the Army portion of the DODIN. CPB also provides the Army with unique, centralized analysis of threat data, trends, forensics, analytic support, and capability requirements. The CPB's two battalions provide 20 CPTs in support of Army and Joint operational forces. Of increasing importance, the Army Reserve and Army National Guard are fielding an additional 21 CPTs. These Compo 2 and 3 forces meet the same training standards as their active duty counterparts and are already contributing to operations.
- ◆ 915<sup>th</sup> Cyber Warfare Battalion (CWB)—Activated at Fort Gordon in 2019, the 915<sup>th</sup> CWB trains and deploys Expeditionary Cyber Teams (ECTs) to augment corps and below formations. ECTs provide offensive Cyber, IO, and EW capability not now fielded to tactical units. At full operating capability, each of 12 ECTs will have organic cyber development capability, network support, and capability to operate independently or as integrated into a supported unit headquarters.

- ◆ 1<sup>st</sup> IO Command (1<sup>st</sup> IOC)—The Army’s only active duty IO brigade, operational since 1994, has initiated a Force Design Update (FDU) that reorganizes the Brigade to increase the number of IO Field Support Teams (FSTs) available, expanding reach-back and social media capability, and adding capacity to support both conventional and Special Operations Forces. By late 2020, 1<sup>st</sup> IOC will also be directly assigned to ARCYBER and continue to provide expert IW planning support to include Operations Security (OPSEC), Military Deception (MILDEC), and IO’s core synchronization and integration functions.
- ◆ Offensive Cyber Operations (OCO) Signal Battalion—ARCYBER has the approval to stand up a long-needed OCO Signal Battalion at Fort Gordon in late 2021, which will provide critical, dedicated support to Army cyber forces and Joint operational missions. The OCO Battalion will be a multi-compo organization, reflecting the critical mission previously performed by Army National Guard Cyber forces as “Task Force Echo.”

**Phase 2—2021-2027, Experiment and Innovate.** Upon consolidating and achieving full operating capability at Fort Gordon, ARCYBER transformation will focus on employing and discovering newly possible operational capabilities enabled by the multiple new capabilities established in Phase 1. As Army commanders gain increased “sets and reps” integrating information capabilities into sustained operations, ARCYBER, in conjunction with TRADOC and Army Futures Command (AFC), will serve as the Army’s key knowledge collector for emerging 21<sup>st</sup> century warfighting art in the IE. Critical initiatives during this phase will include:

- ◆ Information Warfare Operations Center (IWOC)—ARCYBER’s Cyber Operations and Intelligence Center (ACOIC) will continue its transformation to become a full-spectrum IWOC. Featuring multidisciplinary, regionally focused cross-functional teams, the IWOC will give the ARCYBER Commander unprecedented, real-time ability to *sense* and *understand* the global IE, with 24/7 connectivity to all Army Service Component Commands (ASCCs) operational priorities, thereby leveraging the power of centralized visibility for all Army network traffic. This unique vantage point will allow ARCYBER to sense, understand, decide, and respond to emerging global IE conditions, providing options to Army senior leadership and regional Army and Joint Commanders with unmatched speed, enabling strategic decision advantage.
- ◆ Military Intelligence Brigade—Critical to IWOC success and decision advantage will be the establishment of a specialized Military Intelligence (MI) Brigade organic to ARCYBER and focused on the IE, including Cyberspace and the Electromagnetic Spectrum. This not-yet resourced Brigade will partner with the Intelligence Community, AFC, industry, and academia to continually develop, test, and employ cutting-edge technologies (AI, augmented reality, and human-machine interfaces) to analyze the massive data sets by combining traditional all-source intelligence with commercial threat data and open-source information.
- ◆ Network Command (NETCOM) Modernization—To achieve full operating capability, the ARCYBER IWOC will need to transfer many of its current functions to other organizations.



NETCOM, the long-standing strategic Army Signal command that secures, configures, operates, extends, maintains, and sustains the Army portion of the DODIN, is modernizing to take on the Defensive Cyber Operations (DCO) functions now performed by ARCYBER's ACOIC.

- ◆ Joint Force Headquarters Cyber-Army (JFHQ-C (A))—As ARCYBER develops and converges IW capabilities, JFHQ-C(A) (once co-located with ARCYBER Headquarters at Fort Gordon) will immediately benefit and provide enhanced capabilities to USCC missions in support of U.S. Africa Command, U.S. Central Command, U.S. Northern Command, and other missions, as tasked.
- ◆ 780<sup>th</sup> Military Intelligence Brigade (Cyber) – The 780<sup>th</sup> is the Army's offensive cyberspace operations contribution to USCYBERCOM, providing 21 teams in support of National and Combatant Command requirements. In addition, it also maintains the Army's portion of the cyberspace operations infrastructure and owns the Army's Capability Developers, skilled coders whose skills enable both offensive and defensive cyberspace operations. These National Mission Teams and Combat Mission Teams are effects focused; they destroy, degrade, disrupt, deny, and manipulate targets in and through cyberspace. As IW matures, the missions assigned to these teams may shift towards shaping the information environment, particularly as cyberspace operations and operations in all other domains converge to enable MDO.
- ◆ Operational Experimentation—A key focus during Phase 2 will be ARCYBER support to emerging warfighting formations. As the entire Army experiments to develop capabilities that enable MDO, new, innovative formations will emerge. Already in 2020, ARCYBER is providing support to three such mission-specific formations:
  - Multi-Domain Task Force (MDTF)—The MDTF, developed by the Fires Center of Excellence (FCoE), provides an unprecedented long-range fires capability to theater-level commanders. ARCYBER is assisting in training and readiness support to the first MDTF's organic Intelligence, Information, Cyber, Electronic-Warfare, and Space Battalion (I2CEWS BN) that integrates a spectrum of information capabilities to enable long-range targeting.
  - Theater Information Command (TIC)—This Army Futures Command (AFC) concept is for a 2-star, forward-positioned command, providing theater commanders with enduring influence capabilities throughout competition, armed conflict, and consolidation operations. Similar concepts for IW Brigades are emerging from TRADOC for regional collection, analysis, and informational effects-generation formations, focusing full-time on the IE for ASCC and Joint commanders. ARCYBER will robustly support experimenting with these formations during the Joint Warfighting Assessments and DEFENDER exercises.

- Information Warfare Task Force-Afghanistan (IWTF-A)—The Army Special Operations community led the IWTF-A development during combat operations. The IWTF-A was formed in theater, with augmentation from 1<sup>st</sup> IO Command, around a revolutionary operational approach, designed and focused on achieving cognitive effects through the synchronized employment of maneuver forces and information activities. Leveraging hostile fire zone authorities, the IWTF employs Military Information Support Operations (MISO), social media collection, data analytics capabilities, and cutting-edge digital advertising technology to deliver highly effective influence messaging.
- ◆ Army Tactical Force Modernization—ARCYBER is proactively engaged in ongoing modernization efforts to embed appropriate, affordable IW capabilities in ASCC and below formations. Throughout Phase 2, current Cyber-Electromagnetic Activities (CEMA) cells will expand to include increased IO, PSYOP, and Public Affairs personnel, and upgraded capability packages to improve tactical commanders' information capabilities. ARCYBER will build mission-tailored, combined information arms teams to augment maneuver commanders with state-of-the-art, full-spectrum IW capability.
- ◆ Reserve Component Optimization—The overwhelming majority of information capabilities aligned to support conventional forces are found in the reserve component. These include Cyber, IO, Civil Affairs, PSYOP, and Public Affairs formations. Throughout Phase 2, ARCYBER will work to optimize the force structure, composition, and mobilization of Compo 2 and 3 forces to ensure conventional force commanders have the right capabilities to train and influence adversaries during competition.

**Phase 3—2028 and Beyond – Multi-Domain Capable**—By 2028, multiple capabilities and formations identified in 2020 and earlier will come online across the force, greatly enhancing Army commanders' ability to operate in the IE as part of MDO. The ability to conceptualize, design, and execute activities that effectively influence adversary perceptions and actions will be a critical aspect of an MDO-capable Army, particularly in increasingly important, never-renting competition environments. MDO concepts will continue to evolve over the next decade. Already, TRADOC Pam 525-3-1 amply illustrates that information and influence are critical to the three "Competition Actions"<sup>[6]</sup> that Army forces conduct during MDO:

- 1. Enable the Defeat of Information and Unconventional Warfare** — The Army defeats adversary Information Warfare<sup>[7]</sup> by Operations in the Information Environment (OIE).
- 2. Conduct Intelligence & Counter-Adversary Reconnaissance** — This task is fundamentally information and analysis-based, and requires mastery of adversary military capabilities, collecting and analyzing the Operational Environment, including civil networks, and conducting deception.

**3. Demonstrate Credible Deterrent** — Deterrence requires communication. Adversaries obviously will not be deterred by capabilities we have that they do not know about. The Army must establish command and control mechanisms, ensure interoperability, and protect forward presence forces (including cyber and information protection) that achieve deterrence.

As part of the Joint Force, the Army must master these essential Competition Actions through what MDO calls “*active engagement*”<sup>[8]</sup> to become MDO-capable. In each critical task, ARCYBER will play an essential supporting role as the Army better develops its ability to conduct active engagement through the converged employment of maneuver and information capabilities focused on achieving desired cognitive effects and behaviors in our adversaries.

## JOINT OPERATIONAL CONCEPTS

The Joint Force continues to adapt to changes in the OE through the publication of Joint Concepts such as the Joint Concept for Operations in the Information Environment (JCOIE), the Joint Concept for Integrated Campaigning (JCIC), and the Joint Concept for Human Aspects of Military Operations (JC-HAMO).<sup>[9]</sup> These powerful concepts each grapple with varying dynamics of information and how they impact the design and execution of military operations and the use of military force in the emerging Operational Environment. These Joint Concepts are driving better Army concepts, capabilities, and requirements that, in turn, enable Army forces to support Joint Operations in the IE (OIE). For example, in early 2020, the Army Cyber Center of Excellence (CCOE) completed an OIE Force Modernization Assessment (FMA), which generated 33 DOTMLPF-P<sup>[10]</sup> recommendations to mitigate identified gaps in the Army’s IE capabilities. In 2021, the CCOE will produce an AFC-directed Information Functional Concept, which will articulate a long overdue theoretical foundation for viewing information as a military concept and driving doctrinal improvements to posture the Army to win in future competition and conflict.

## CONCLUSION

When we look back as an MDO capable force, 2020 will stand out as a pivotal year for Army Cyberspace, EW, and IO forces. After decades of dabbling in tactical IO, the Army undertook a sweeping series of robust modernization efforts to dramatically transform ARCYBER to better enable commanders across the Army with the ability to sense, understand, decide, act and assess faster than our competitors and adversaries, gaining critical decision advantage in an era of information warfare. 🛡️

**NOTES**

1. General James C. McConville, 40<sup>th</sup> Chief of Staff of the U.S. Army, [https://www.army.mil/article/225605/40th\\_chief\\_of\\_staff\\_of\\_the\\_army\\_initial\\_message\\_to\\_the\\_army\\_team](https://www.army.mil/article/225605/40th_chief_of_staff_of_the_army_initial_message_to_the_army_team).
2. Joint Pub 3-13, 2014, U.S. Joint Doctrine defines the Information Environment as “the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.”
3. Information Warfare is not a doctrinally defined term. Further, the acronym “IW” within DOD commonly connotes Irregular Warfare. In this article, “IW” refers only to the concept of information warfare, as described in the text.
4. Army Regulation (AR) 10-87, Army Commands, Army Service Component Commands, and Direct Reporting Units, 2188 Washington, DC: Government Printing Office, 2017, para 14-2, 17, details 10 specified tasks that are here grouped for clarity as three major functions.
5. The Army Modernization Strategy, [https://www.army.mil/standto/archive\\_2019-10-17/](https://www.army.mil/standto/archive_2019-10-17/).
6. TRADOC Pamphlet 525-3-1, The U.S. Army in Multi-Domain Operations, Fort Eustis, VA: US Army Training and Doctrine Command, 2018, <https://adminpubs.tradoc.army.mil/pamphlets.html>, 27.
7. The MDO concept internally defines IW as an enemy activity, see p. GL-6: “Employing information capabilities in a deliberate disinformation campaign supported by actions of the intelligence organizations designed to confuse the enemy and achieve strategic objectives at minimal cost.”
8. TRADOC Pamphlet 525-3-1, para 3-5b, 27.
9. Joint Concepts, <https://www.jcs.mil/Doctrine/Joint-Concepts/Joint-Concepts/>.
10. Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy, <http://acqnotes.com/acqnote/acquisitions/dotmlpf-analysis>.





# 16<sup>th</sup> Air Force and Convergence for the Information War

---

Lieutenant General Timothy D. Haugh

Lieutenant Colonel Nicholas J. Hall

Major Eugene H. Fan

**T**he world has changed, and our approach to warfare must change with it. As traditional organized power structures erode, disorder fills the void. We are moving from successive regional conflicts to a future characterized by continual global competition. This circumstance will reward those who can leverage information for strategic advantage. The 2018 National Defense Strategy (NDS) described this new paradigm by emphasizing the need to compete with adversaries now.<sup>[1]</sup> The Air Force recognizes that we are already in competition below the threshold of armed conflict. Within the Air Force, the standup of 16<sup>th</sup> Air Force as an Information Warfare (IW) Numbered Air Force (NAF) in October 2019 represents a direct response to this new reality. In the document directing the standup, the Air Force described IW as “The employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior.”<sup>[2]</sup> Our task is to synchronize – Cyberspace; Intelligence, Surveillance, and Reconnaissance (ISR); Electromagnetic Warfare (EW); Information Operations (IO) – across the continuum of cooperation, competition, and conflict, and support the joint force’s ability to compete, deter, and win wars across multiple domains.<sup>[3]</sup>

Within the 16<sup>th</sup> Air Force, IO describes a collection of activities to include Military Information Support Operations (MISO), Military Deception (MILDEC), Operations Security (OPSEC), and Audience Engagement. We intend to synchronize all 16th Air Force capabilities and activities through a unifying approach of convergence. We define convergence as *the integration of capabilities that leverage access to data across separate functions in a way that both improves the effectiveness of each functional capability and creates new information warfare outcomes*. This builds on the U.S. Army concept of convergence that focuses on enabling tactical multi-domain effects during combat, by emphasizing competition and synchronizing effects in the information environment. In this article, we describe

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



**Lt Gen Timothy D. Haugh** is the Commander, Sixteenth Air Force, Commander, Air Forces Cyber, and Commander, Joint Force Headquarters-Cyber, Joint Base San Antonio-Lackland, Texas. Lt Gen Haugh is responsible for more than 44,000 personnel conducting worldwide operations. The general leads the global information warfare activities spanning cyberspace operations, intelligence, targeting, and weather for nine wings, one technical center, and an operations center. Previously, he was Commander of the Cyber National Mission Force, where he coordinated the prevention and response to cyber incidents and campaigns perpetuated by threat actors in order to preserve U.S. critical infrastructure and key resources. Lt Gen Haugh is a graduate of Lehigh University in Bethlehem, Pennsylvania, and holds Master's degrees from Southern Methodist University, Naval Postgraduate School, and the Industrial College of the Armed Forces.

how competition in the 21st-century necessitates a change in our approach to warfighting. Next, we discuss why 16<sup>th</sup> Air Force was stood up in response to this change and our approach to IW. Finally, we introduce the concept of convergence as a framework for how to compete in the information environment on a flexible but global scale.

## COMPETITION AND THE RESULTING IMPERATIVE

Our adversaries have brought strategic competition to the nation's front door by engaging the United States' (US) population in the information environment. Russia and China have sought to create distrust in the US and allied political, military, and economic institutions and processes. Our adversaries' goal is to degrade political will or to generate internal conflict, while creating the plausible deniability necessary to avoid international responsibility.<sup>[4]</sup> As state and non-state actors rapidly evolve IW capabilities to control the narrative surrounding their actions, they are redefining what "combined arms" means in 21st-century warfare.<sup>[5]</sup>

In 2016, Internet trolls working for the Russia-based Internet Research Agency (IRA) exploited social media to target the US electoral process in an IW campaign designed to spread disinformation, create distrust, and increase societal division.<sup>[6]</sup> However, Russia's malign influence stretches well beyond the US. The Kremlin's efforts to influence political outcomes span the globe, ranging from political financing, to private military corporations, to special operations activities on nearly every continent.<sup>[7]</sup>

More recently, China leveraged the COVID-19 pandemic to expand its influence through a full-spectrum of IW activities. To deflect perceptions that it was mishandling the initial stages of the COVID-19 outbreak, China initiated a "global coronavirus rescue campaign," focused on sending aid packages to European Union nations. China aggressively publicized this effort while





Lt Col Nicholas J. Hall is the Director of the Commander's Action Group, Sixteenth Air Force /Air Forces Cyber. A career intelligence officer, Lt Col Hall was previously the Director of Operations for the 15<sup>th</sup> Intelligence Squadron, Joint-Base Langley-Eustis, Virginia. He has served as an analyst in the U.S. Central Command and U.S. Pacific Command areas of responsibility, as an intelligence crew member in an Air Force Special Operations Command MQ-1B unit, and has held three targeting positions at the squadron, major command, and combatant command level. He has also deployed to the Combined Air Operations Center in Southwest Asia and to Afghanistan, where he was a U.S. Army cavalry squadron S2. Lt Col Hall is a graduate of Baylor University in Waco, Texas, holds a Master's degree from American Military University, and is a distinguished graduate of the U.S. Air Force Air Command and Staff College.

simultaneously blaming the US for causing the pandemic.<sup>[8]</sup> Some observers have noted that China's information strategy surrounding the pandemic appears similar to the Russian playbook of spreading disinformation to create doubt about established facts.<sup>[9]</sup> Our adversaries employ integrated approaches, combining messaging in the media with economic pressure, military maneuvers, and diplomacy to impose a cost. The US must expand and broaden our own competition globally in the information environment while remaining consistent with our values built on a "foundation of mutual respect, responsibility, priorities, and accountability" with our allies as outlined in the NDS.<sup>[10]</sup>

As US adversaries increasingly pull the multidisciplinary levers of IW, the information environment gives them global access to compete at a low cost. In a globalized data-age, the outcomes of these actions are not constrained to segmented geographic regions. Department of Defense (DoD) leaders have recognized this threat. The Chairman of the Joint Chiefs of Staff has pushed the joint force toward globally integrated campaigns and exercises to operationalize cross-combatant command coordination on global problem sets.<sup>[11]</sup> However, this transformation will not happen overnight. Joint force commanders are demanding options below the level of armed conflict, and plans that integrate multi-domain capabilities and creatively leverage IO. As the DoD explores options to increase competition, we must look for new ways to partner across U.S. Government departments and agencies. If we want to gain the initiative in the information environment, we need a new approach to warfighting.

## THE RESPONSE – WHY 16<sup>TH</sup> AIR FORCE WAS ESTABLISHED

Since 9/11, the joint force approach to warfighting has been shaped by the conflict against violent extremism. The Air Force ISR enterprise and the



**Maj Eugene H. Fan** is the Aide-de-Camp to the Commander, Sixteenth Air Force/Air Forces Cyber. A career logistician and aircraft maintenance officer, Maj Fan has held various positions to include Operations Officer, Executive Officer, and Officer-in-Charge at multiple echelons and maintenance organizations. Prior to his current position, Maj Fan was the Chief of the Maintenance Operations Branch, Headquarters Twenty-fifth Air Force, Joint Base San Antonio-Lackland, Texas. He has also deployed as an Operations Officer to Southwest Asia, where he led the generation of strike, intelligence and reconnaissance, aeromedical evacuation, and command and control missions in support of several operations in the theater. Maj Fan is a graduate of the University of Georgia in Athens, Georgia, holds a Master's degree from Oklahoma University in International Relations, and is a graduate of the Air Force's Advanced Maintenance and Munitions Operations School.

Intelligence Community more broadly optimized collection, analysis, and reporting strategies to enable find-fix-finish operations against single or small groups of combatants on the battlefield. The target development required to establish a pattern of life, distinguish between combatants and non-combatants, and achieve positive identification of the enemy was enabled by time-intensive and overlapping collection in a permissive environment. For example, the 2006 strike on Abu Musab al-Zarqawi took “600 hours of Predator time and thousands of hours of analyst time to facilitate a strike executed in a matter of minutes.”<sup>[12]</sup> In this environment, the joint force developed a series of command and control processes that synchronized ISR and EW capabilities to efficiently find and fix a homogenous adversary. Those processes were not constrained by time, and they were geographically bounded. Additionally, cyberspace and IO capabilities were rarely used as either a primary effects mechanism or as a collection enabler. This model was sufficient for its time and place. However, to effectively respond to inter-state competition from Russia and China, the joint force must better integrate IW capabilities and employ a process that is relevant to the speed of the information environment. Within the Air Force, previous approaches to ISR strategies for great power competition; the integration of Cyber, IO, and EW; and command and control of these capabilities fell short.

Russia's annexation of Crimea in 2014 was achieved using a combination of armed force, deception, IO, criminal activity, and political and economic actions.<sup>[13]</sup> Russia's strategy – what some have termed the “Gerasimov doctrine,” for Russia's Chief of the General Staff General Valery Gerasimov – blurs “the line between a state of war and peace” and employs “extensive use of political, economic, diplomatic, information, and other nonmilitary measures, all supported by the protest potential of a population.”<sup>[14]</sup> At the time, the North Atlantic Treaty Organization

(NATO) Supreme Allied Commander Europe, General Philip Breedlove, admitted that “the actions of Russia and its leadership are extremely difficult to predict.”<sup>[15]</sup> This difficulty resulted in part because military service and Intelligence Community capabilities were positioned to assess Russian actions as indications and warning predictors within a traditional “conception of conflict.”<sup>[16]</sup> Orienting joint force capabilities in this way creates a “curtain of ambiguity,” limiting insights into adversary intent and complicating the identification and discrimination of targets in the information environment. In 2014, the DoD was seemingly unprepared to offer any IW response.

To respond effectively to similar scenarios in the future, the Air Force must adopt an approach that enables a clear focus on these hard problems. This approach should take a global viewpoint and use access to data across each IW capability to generate insights into the adversary’s whole-of-nation approach to strategic competition. It must not only effectively integrate capabilities to produce timely effects in the information environment, but it should also enable partners across the DoD, U.S. Government departments and agencies, and foreign partners to counter a present and growing threat. The Secretary of the Air Force established the 16<sup>th</sup> Air Force for this reason; to specifically converge these capabilities and activities in the information environment.

Convergence on priority problems positions the 16<sup>th</sup> Air Force to enable combatant commands and air components to create IW outcomes in globally integrated campaigns. Outcomes are results that directly achieve a commander’s objective. Within the context of strategic competition, these can range from using cyber effects to deny or degrade an adversary’s operations, precision messaging that leverages deception to affect individual or unit behavior, a public affairs release that exposes malign activity, Treasury Department (USDT) sanctions, State Department (DOS) demarches, and other means. While the Air Force has enabled some of these outcomes previously, our service was not postured to generate these IW outcomes in a timely, consistent, or synchronized manner. The order establishing the 16<sup>th</sup> Air Force succinctly describes the challenge highlighted in the preceding paragraphs: “The separation of Cyber, Intelligence Surveillance and Reconnaissance (ISR), Electronic Warfare (EW), and Military Information Support Operations (MISO)/Military Deception (MILDEC) among different organizations coupled with an inability to integrate multi-domain operational and tactical activities puts the Air Force at a disadvantage across the conflict continuum.”<sup>[17],[18]</sup> The 16<sup>th</sup> Air Force is charged with integrating these capabilities, and will leverage a unique global vantage point to generate insights on adversary activity that lead to outcomes that make us competitive now.

Convergence in the information environment integrates capabilities by combining cross-functional data and tradecraft in creative ways, ultimately generating outcomes greater than each individual capability can create on its own. As the 16<sup>th</sup> Air Force builds towards convergence, we must articulate our approach to IW as a command, how we operationalize convergence, and examine how convergence applies to, and changes, warfighting.

## INFORMATION WARFARE FOUNDATION

The 16<sup>th</sup> Air Force IW outcomes are built on three foundational lines of effort: Generate Insights, Compete Now, and Prepare for Escalation.

**Generate Insights.** All warfighting activities center on understanding the adversary. The 16<sup>th</sup> Air Force is uniquely positioned within the joint force to continuously generate insights across a spectrum of activities now integrated into an IW force. These include Signals Intelligence (SIGINT) missions as delegated by the National Security Agency (NSA), medium-and high-altitude ISR collection as tasked by air components, problem-centric analysis and exploitation through the Distributed Common Ground System (DCGS) enterprise, robust reach-back analysis and targeting enterprise, insights derived from operations in cyberspace, and insight into adversary mindset from behavioral science resources.

Two factors within this line of effort complicate a transition to converged IW. The first is that in the information environment, battlespace awareness often looks different from the traditional Intelligence Preparation of the Operational Environment (IPOE), which focuses on the order of battle of physical targets and decision support. While these activities must continue, we need to think differently. This will require new tradecraft to recognize and counter threats, and may involve new data sources, collection strategies, and methods of analysis to create outcomes in the information environment. Second, the need to improve data integration among intelligence capabilities increases as we shift to global challenges that affect traditional geographic and functional areas of responsibility. Units within our enterprise will require tight integration to rapidly incorporate insights generated across multiple disciplines. Convergence addresses the various functional Air Force data stovepipes that have formed over the last two decades.

**Compete Now.** The implementation of convergence will be marked by a cultural shift across the Air Force. We must begin to expose adversary activities that seek to undermine the US position and destabilize the international order. U.S. Africa Command (USAFRICOM) took this initiative on May 26, 2020, when it publicly released unclassified imagery of Russian MiG-29 and Su-24 aircraft deployed to Libya. In a statement amplified by CNN, USAFRICOM disclosed that “Moscow recently deployed military fighter aircraft to Libya in support of Russian state-sponsored private military contractors operating on the ground there.”<sup>[19]</sup> The aircraft had also been painted to remove national markings. The USAFRICOM exposure of Russian malign action is an IW outcome the 16<sup>th</sup> Air Force should regularly enable by generating the initial insights into the adversary activity and shaping the information environment to counter adversary actions.

U.S. Cyber Command (USCYBERCOM) has also advanced joint force thinking on competition through General Paul Nakasone’s concept of Persistent Engagement. This concept implements the 2018 DoD Cyber Strategy, which explains that contact with adversaries in cyberspace is continuous. Thus, it is appropriate to “defend forward” and engage militarily in this domain to

protect our national interests.<sup>[20]</sup> Indeed, the 2019 National Defense Authorization Act (NDAA), embraces this strategy by defining operations in cyberspace as a “traditional military activity.”<sup>[21]</sup> A similar shift has started within the information environment but must accelerate more broadly. Leveraging not only cyberspace but all IW capabilities, 16<sup>th</sup> Air Force must converge on the nation’s highest priority problems. This process will yield outcomes for the joint force or options for partners within the U.S. Government to execute multi-domain IW operations against our adversaries.

Producing an outcome in the information environment does not always require DoD action; other government departments and agencies often bring unique authorities and approaches. For example, some outcomes can result from a USDT sanction, a Department of Justice (DOJ) indictment, or enabling DOS to work through a partner nation. Such partnerships led to the March 2018 USDT sanctions against five entities and nineteen individuals for “interference in U.S. elections, destructive cyber-attacks, and intrusions targeting critical infrastructure.”<sup>[22]</sup> This approach can enable the full power of the U.S. Government to achieve strategic outcomes.

Multi-domain and whole-of-government IW operations will impose a cost on US adversaries by exposing their malign activity and eliminating their plausible deniability.<sup>[23]</sup> This approach will force adversaries to respond, expend resources internally, or change their strategies. The Air Force has many of the resources required to compete persistently in the information environment, which is an NDS imperative. We now need an approach that accelerates action. As 16<sup>th</sup> Air Force aligns on priority targets for competition, the challenge will be to synchronize the activities required to produce effective outcomes inside our adversaries’ OODA loop—Observe-Orient-Decide-Act.<sup>[24]</sup>

**Prepare for Escalation.** As 16<sup>th</sup> Air Force expands its options to compete, we must remain ready for conflict escalation. We must continue to perform each IW capability with excellence and be ready to support joint force commanders in the event of a conflict. The 16<sup>th</sup> Air Force approach to IW should also include strategies that impose cost and deter escalation without provoking it. Additionally, US adversaries should be mindful that IW outcomes can rapidly shift along the competition continuum.<sup>[25]</sup> The intelligence and targeting data used to generate outcomes that compete with our adversaries in the information environment can be applied to produce non-kinetic or kinetic outcomes if the conflict escalates.

Conflict with a peer adversary will be characterized by several complicating factors, including, the “geographic asymmetry” posed by our force posture relative to China and Russia, and an increased number of adversary targets on the battlefield.<sup>[26]</sup> Our adversaries will employ a range of offensive standoff weapons to deny access as well as “semi-autonomous unmanned aircraft, drone submersibles, small vessels, and smart mines” to complicate effective maneuver.<sup>[27]</sup> Additionally, China and Russia will target<sup>[27]</sup> our most critical capabilities, including the network and communications infrastructure, which the joint force relies on for command and control.

To win in this environment, 16<sup>th</sup> Air Force must deliver a range of kinetic and non-kinetic outcomes. Effective IW operations in a peer conflict will require tight synchronization among ISR, Cyber, EW, and IO, as well as seamless integration into combatant command operational processes. Future battlespace conditions will expand the distance but limit the time required to find, fix, and finish targets. Accordingly, the data produced by each IW capability must be automatically accessible and integrated into all nodes in the kill chain both vertically and horizontally. The Joint All Domain Command and Control (JADC2) concept linking all sensors to all shooters describes this approach.<sup>[28]</sup> In addition to the material means required to achieve this level of integration, we must shift “our doctrinal dependence on large vulnerable centralized command and control nodes to more agile, networked solutions.”<sup>[29]</sup> Our IW forces must integrate into joint command and control concepts that allow for the flexible employment of a distributed force. The speed of decision required to respond to a peer adversary in a dynamic tactical situation will require ISR, EW, IO, and offensive and defensive cyber Airmen to repeatedly make decisions and execute distributed operations under mission command with limited direction from higher headquarters. The possibility of such a scenario requires 16<sup>th</sup> Air Force to maintain excellence across its IW capabilities, and the convergence of our forces in the information environment will now prepare us to seamlessly integrate in a future conflict.

## **CONCEPTUALIZING CONVERGENCE**

The 16<sup>th</sup> Air Force is building an approach to IW by tailoring the Army’s concept of convergence to our enterprise. We will operationalize convergence by both commanding and controlling our assigned forces, and enabling the horizontal awareness among tactical units required to synchronize the broader enterprise at the operational level of war. To succeed, we must acknowledge and overcome several historical biases and thereby rapidly transition to a problem-centric approach that leverages 16<sup>th</sup> Air Force global operations, authorities, and access to data.

The U.S. Army’s Multi-Domain Operations (MDO) doctrine defines convergence as “the rapid and continuous integration of capabilities in all domains, the electromagnetic spectrum, and the information environment that optimizes effects to overmatch the enemy through cross-domain synergy and multiple forms of attack all enabled by mission command and disciplined initiative.”<sup>[30]</sup> The Army’s concept prescribes the need for data from any sensor to flow through any command and control node to enable any shooter, which is critically important, especially at the tactical level. The Air Force IW enterprise is service-unique, so we have built upon the Army’s foundational work. As 16<sup>th</sup> Air Force expands convergence to address strategic competition, we must address some long-standing biases that could impact how we compete effectively on a global scale.

### ***Bias 1 – Geographic Organization and Outlook***

Geographic boundaries pose no constraints for data and information; our IW outcomes should also be unconstrained. China and Russia do not operate in accordance with joint force command boundaries—they are global malign actors whose exploitation of the information environment impacts every combatant command. A Strategic Multilayer Assessment (SMA) White Paper released by the Joint Staff in May 2019 assessed Russia would increase its “gray zone” tactics across Europe and Central Asia, Africa, the Middle East, the US, and Latin America in the near term.<sup>[31]</sup> 16<sup>th</sup> Air Force capabilities are distributed globally and have an array of vantage points into each of those regions. To leverage the unique capabilities of our global enterprise, we must capitalize on the agility such a distributed force offers. In many cases, the Airmen working to develop an outcome might not be “owned” by or even reside within, a given command with authority to execute IW operations—they must instead work seamlessly with a command that does. The more globally integrated the joint force becomes, the more natural this will seem. We envision scenarios wherein the same commander can alternate between supported and supporting during the same operation, or simultaneously exist in both states.

### ***Bias 2 – Command and Control Blinders***

Command and control are essential to the efficient and disciplined execution of combat operations. At all levels of war, the joint force requires clear lines of command responsibility. However, if we only shoot, move, and communicate with those elements directly in our chain of command, we are less agile, less informed, miss opportunities, and are vulnerable to exploitation. Convergence does not require a change in command and control doctrine. What we need is a new framework that organizes global synchronization at the speed of IW.

### ***Bias 3 – Focus on Conflict***

We must always be prepared for armed conflict, but our adversaries are out-competing us now. The Secretary of Defense, Dr. Mark Esper, put it this way in a December 2019 press briefing: “We must deal with the world we live in, not the one we want.”<sup>[32]</sup> While US adversaries’ actions are at times escalatory, they fall below the threshold of armed conflict. They cannot act with complete impunity, yet their manipulation of the information environment clouds the truth, redirects blame, or creates plausible deniability that inoculates them against international consequences. Through these incremental gains, they achieve strategic ends without the need for war. There is a growing demand from combatant commanders to shift military service weight of effort toward outcomes that regain the initiative in the information environment.

## **OPERATIONALIZING CONVERGENCE**

Implementing convergence in the information environment requires new operational art. Our framework starts within the 16<sup>th</sup> Air Force to synchronize outcomes on common operational priorities that cross combatant command boundaries. These outcomes address

problems that, in many cases, are being simultaneously requested and prioritized across combatant commands. Russian malign influence impacts each geographic and functional combatant command in the DoD. However, legacy, stovepiped processes, and data access all limit awareness and collaboration both inside 16<sup>th</sup> Air Force, and among component and combatant command staffs that are divided by geographic boundaries.

Convergence is designed to leverage both existing command and control constructs that direct forces and activities while enabling synchronization among partners that leads to mutually beneficial outcomes for multiple commanders. Ultimately, we will realize convergence by leveraging the inherent strengths of the 16<sup>th</sup> Air Force outlined below.



Figure 1. Convergence Formula

First, 16<sup>th</sup> Air Force is *problem-centric* and has moved away from a platform or sensor-based approach to one that leverages access to many data sources, regardless of origin. This approach allows our Airmen to gain insights that improve the understanding of the adversary and solve the most important operational problems for joint force commanders.

Second, 16<sup>th</sup> Air Force has *access to data* across each IW function. Integrating this data into a combined picture provides a global vantage point. As a result, the problem-centric approach becomes unconstrained by geographic boundaries and provides the opportunity to generate global outcomes.

Third, the 16<sup>th</sup> Air Force is assigned *authorities* unique within the Air Force, that include roles as the Service Cryptologic Component to the National Security Agency (NSA), a Component-Numbered Air Force (C-NAF) within Air Combat Command, a Service Cyber Component in Combatant Command relationship to USCYBERCOM and in general support to four other Combatant Commands, and as the operational commander of the Air Force Information Network (AFIN). The 16<sup>th</sup> Air Force will leverage these authorities to take full advantage of the elements we command and control in cyberspace operations, the enterprise data access inherent to each line of authority, and the broader capacity of our ISR, targeting, and EW capabilities.



Additionally, the partnerships we have built with air components, combatant commands, and within the interagency, enhance the effectiveness of 16<sup>th</sup> Air Force capabilities. This powerful combination will enable new global IW outcomes, either in the form of options for a supported joint force commander or as an outcome 16<sup>th</sup> Air Force creates as the supported component to compete in the information environment.

The 16<sup>th</sup> Air Force is tasked both with developing the partnerships that bring alignment and enable the horizontal awareness required to achieve problem-centric collaboration and data integration. This results in two byproducts. First, as we increase data sharing, each functional capability will gain additional insights that improve analysis, signal development, and follow-on collection. Second, as the operational staff synchronizes previously stovepiped capabilities on global problems, we will create new IW outcomes not previously realized within the Air Force. We expect many of these to be fact-based public disclosures. This is our comparative advantage, and it is an approach to convergence that has not yet been executed to the scale we envision.

## **SELECTED WARFIGHTING APPLICATIONS FOR CONVERGENCE IN THE INFORMATION ENVIRONMENT**

Our approach to convergence will address several sets of problems within the information environment. The below examples are not all-inclusive but demonstrate a range of possible outcomes that allow us to compete against our adversaries now. A brief examination of these examples reveals opportunities to leverage our access to data, authorities, and partnerships. As 16<sup>th</sup> Air Force initiates operations, we begin to see the value of converged IW outcomes.

**Countering Disinformation.** We will quickly realize the potential for convergence in our mission to counter disinformation. Our adversaries aim to supplant logic and fact with fantasy and fear by saturating the information environment with lies.<sup>[33]</sup> We counter this by adhering to the inherent strengths and core values of our nation—we speak the truth. As the US military shifts its focus to this societal threat, our ability to generate insights postures the 16<sup>th</sup> Air Force well for this challenge.

Today, Joint Force Headquarters cyber teams are developing options to impose a cost on adversaries who inject disinformation into the environment. Additionally, our DCGS enterprise is employing a problem-centric approach to gain a deep understanding of adversary malign activity in support of air components. Our cyber defense Airmen are exposing malign cyber activity, while our global targeting wing has focused target systems analysis and non-kinetic intelligence analysis on malign adversary influence. Simultaneously, four wings across the 16<sup>th</sup> Air Force ISR enterprise are leveraging Publicly Available Information (PAI) to gain insight and develop tradecraft to expose a similar activity.

As we connect and share data among these functional capabilities, each unit will improve the quality of insights it can provide to the tasking command. Additionally, as the 16<sup>th</sup> Air Force IW Operational Staff organizes the converged approach, planners will identify new outcomes that can be generated by taking a global view of the data generated by each subordinate unit. Some outcomes might be precise and enabled by cyber. In other cases, our operationalized Public Affairs elements will be best suited to counter disinformation with the truth. Both options impose a cost on the adversary by either compelling a change in behavior or deterring a future action. Most importantly, we must recognize that what sets us apart from our adversaries is that rather than spreading disinformation, we deal in truth. The Air Force can be aggressive within the information environment because we will produce facts and fact-based evidence of malign activity. Convergence creates a framework that enables the 16<sup>th</sup> Air force to begin injecting that truth into the information environment at an unprecedented speed and scale.

**Cyber-Enabled Information Operations.** By integrating our Joint Force Headquarters cyber teams with our growing IO force, we can scale to create effects against targets where combatant commanders currently lack options. Alignment of our ISR collection and analysis units against these targets will also yield intelligence and cultural insights that our IO professionals can use to increase target fidelity and create behavioral change. For example, Joint Task Force (JTF) ARES achieved this against the Islamic State of Iraq and Syria (ISIS). JTF ARES integrated multiple disciplines to create confusion and distrust within ISIS and ultimately worked closely with partners to dismantle its web-based operations.<sup>[34]</sup>

Cyberspace access will be essential to creating precision effects in the information environment. Precision effects will also be somewhat of a cultural shift in military operations, which has often focused on messaging aimed at more generalized populations. Precision, cyber-enabled IO, provides an intermediate option between broad messaging and a kinetic strike. It may enable more predictable effects and, in some cases, lower cost, and pose a lower risk to escalation. Regardless of the use case, tight synchronization among units working across the information environment is required to converge effectively against global targets.

**Convergence in Space.** The 16<sup>th</sup> Air Force (Air Forces Cyber (AFCYBER)) was recently designated the cyber component in general support to U.S. Space Command (USSPACECOM). With the standup of the U.S. Space Force (USSF), we must consider what IW looks like in this domain. In the coming decades, space will become more accessible and consequential to the civil, military, and economic interests of all nations. As this happens, states will correspondingly increase competition in and through space.<sup>[35]</sup> No domain lends itself to the synergy of cyber, ISR, EW, and IO like space. A converged approach to IW in support of USSPACECOM should leverage these mutually supportive capabilities to rapidly generate outcomes.

USSPACECOM has recently demonstrated clear initiative in responding to adversary space activity. Russia's direct ascent anti-satellite missile test on April 15, 2020, represents a clear threat to the global community and undermines Russia's advocacy for a treaty banning weapons

in space. In response, the Commander of USSPACECOM, General Jay Raymond, publicly stated, “This test is further proof of Russia’s hypocritical advocacy of outer space arms control proposals designed to restrict the capabilities of the United States while clearly having no intention of halting their counter-space weapons programs.”<sup>[36]</sup> He later responded to Iran’s failed attempt to employ an imaging satellite by tweeting information regarding the failure derived from USSPACECOM space-tracking capabilities.<sup>[37]</sup> As adversaries increase competition in and through space, an IW posture such as the one demonstrated by the USSF will enable rapid outcomes that position the nation for continued ascendancy over strategic rivals in space.

## CHANGING THE WAY WE FIGHT

To effectively compete at scale, we need an approach to IW that builds on US strengths and values. IW requires tight partnerships among all elements of the DoD, the interagency, and our coalition partners, driving a shift in the weight of effort from preparing for conflict to competing now. As military leaders, this is an opportunity to re-evaluate historical biases that constrain us from competing in the information environment. We do not need a new approach to command and control, but a new framework that both materially creates the awareness *among*, and organizes the horizontal coordination *of*, organizations across the continuum of cooperation, competition, and conflict. The NDS is driving the DoD to examine competition through a new lens. We believe the creation of 16<sup>th</sup> Air Force and our approach to convergence in the information environment offers new opportunities to compete now. As the 16<sup>th</sup> Air Force enters full operational capability in 2020, we are taking a problem-centric approach to competition. Our global vantage point, enabled by access to data and authorities, will improve each of our capabilities while producing new IW outcomes through operations that will be simultaneously supported and supporting. We are confident this approach will change the way the Air Force fights.🛡️

## NOTES

1. Department of Defense, *Summary of the 2018 National Defense Strategy of the United States of America*, Washington, DC: Department of Defense, 2018, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
2. Headquarters United States Air Force, Program Guidance Letter (PGL) 19-05, *Establishment of the Information Warfare (IW) Component Numbered Air Force (C-NAF) under Air Combatant Command*, September 6, 2019, 5.
3. Department of Defense, *Joint Doctrine Note 1-19: Competition Continuum*, Washington DC: Department of Defense, 2019, [https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn\\_jg/jdn1\\_19.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf).
4. Sean McFate, *The New Rules of War: Victory in the Age of Durable Disorder*, William Morrow, 2019.
5. Department of Defense, *Strategy for Operations in the Information Environment*, Washington DC: Department of Defense, 2016, <https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf>.
6. Department of Justice, *Report on the Investigation Into Russian Interference In the 2016 Presidential Election*, Washington DC: Department of Justice, 2019, <https://www.justice.gov/storage/report.pdf>.
7. Tim Lister, Sebastian Shukla, and Clarissa Ward, "Putin's Private Army." CNN. Cable News Network, 2019, <https://www.cnn.com/interactive/2019/08/africa/putins-private-army-car-intl/>.
8. "Is China Winning the Coronavirus Response Narrative in the EU?" Atlantic Council, March 26, 2020, <https://www.atlanticcouncil.org/blogs/new-atlanticist/is-china-winning-the-coronavirus-response-narrative-in-the-eu/>.
9. Jessica Brandt and Bret Schafer, "Five Things to Know About Beijing's Disinformation Approach." Alliance For Securing Democracy, April 1, 2020, <https://securingdemocracy.gmfus.org/five-things-to-know-about-beijings-disinformation-approach>.
10. Department of Defense, Summary of the 2018 National Defense Strategy of the United States of America, Washington, DC: Department of Defense, 2018, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.
11. Jim Garamone, "Global Integration Deserves More Attention, Selva Says." U.S. DEPARTMENT OF DEFENSE, June 19, 2019, [www.defense.gov/Explore/News/Article/Article/1881159/global-integration-deserves-more-attention-selva-says/](http://www.defense.gov/Explore/News/Article/Article/1881159/global-integration-deserves-more-attention-selva-says/).
12. Robert Haffa and Anand Datla, "Joint Intelligence, Surveillance, and Reconnaissance in Contested Airspace," *Air And Space Power Journal*, May-Jun (2014): 31, [https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-28-Issue-3/F-Haffa\\_Datla.pdf](https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-28-Issue-3/F-Haffa_Datla.pdf).
13. John Davis Jr., "Continued Evolution of Hybrid Threats: The Russian Hybrid Threat Construct and the Need for Innovation," *The Three Swords Magazine* 28 (2015): 23, [http://www.jwc.nato.int/images/stories/threeswords/CONTINUED\\_EVOLUTION\\_OF\\_HYBRID\\_THREATS.pdf](http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf).
14. Timothy Thomas, "Russian Military Thought: Concepts and Elements," *Report sponsored by U.S. European Command*, (McLean, VA: MITRE Corporation, 2019), 11-13, <https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf>.
15. Lysgard Asbjorn and Boye Lillerud, "How is Russian Hybrid Warfare a Challenge to the Intelligence Function at the Operational Level and to What Extent Should it Adapt," *Arts and Social Sciences Journal* 10, no. 3 (2019), 2, [https://astonjournals.com/manuscripts/Vol\\_10\\_2019/ASSJ\\_Voll0\\_3\\_how-is-russian-hybrid-warfare-a-challenge-to-the-intelligence-function-at-the-operational-level-and-to-what-extent-shoul.pdf](https://astonjournals.com/manuscripts/Vol_10_2019/ASSJ_Voll0_3_how-is-russian-hybrid-warfare-a-challenge-to-the-intelligence-function-at-the-operational-level-and-to-what-extent-shoul.pdf).
16. Frank Hoffman, "On Not-So-New Warfare: Political Warfare Vs. Hybrid Threats," *War on The Rocks*, July 2014, <https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/>.
17. Headquarters Air Combat Command Planning Order (PLANORD) 19-001, *Optimization of ACC Information Warfare (IW) Force Generation and Presentation*, April 3, 2019, 1.
18. Department of Defense, *Joint Publication 3-13: Information Operations* (Washington DC: Department of Defense, 2014), 34-35, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_13.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf).
19. Ryan Browne and Gul Tuysuz, "US military accused Russia of deploying fighter aircraft to Libya." CNN.com. <https://www.cnn.com/2020/05/26/politics/russia-fighter-aircraft-libya/index.html>, accessed May 27, 2020.
20. Department of Defense, *Summary of the Department of Defense Cyber Strategy*, Washington DC: Department of Defense, 2016, [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER\\_STRATEGY\\_SUMMARY\\_FINAL.PDF](https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF) 2018.

## NOTES

21. National Defense Authorization Act for fiscal year 2019: conference report, Washington, D.C.: U.S. G.P.O.
22. Department of the Treasury. *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks*: Press Release on March 18, 2018, <https://home.treasury.gov/news/press-releases/sm0312>.
23. Sean McFate, *The New Rules of War: Victory in the Age of Durable Disorder*.
24. David S. Fadok, *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis*, Air University Press, (Maxwell AFB, AL, February 1995), 16, [http://dtlweb.au.af.mil/webclient/treamGate?folder\\_id=0&dvs=1590791287782-577](http://dtlweb.au.af.mil/webclient/treamGate?folder_id=0&dvs=1590791287782-577).
25. Department of Defense, *Joint Doctrine Note 1-19: Competition Continuum* (Washington DC: Department of Defense, 2019), [https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn\\_jg/jdn1\\_19.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf).
26. Michael Mazarr, "Toward a New Theory of Power Projection," *War on The Rocks*, April 2020, <https://warontherocks.com/2020/04/toward-a-new-theory-of-power-projection/>.
27. *Ibid.*
28. Morgan Dwyer, "Making the Most of the Air Force's Investment in Joint All Domain Command and Control," Center for Strategic International Studies, March 2020, <https://www.csis.org/analysis/making-most-air-forces-investment-joint-all-domain-command-and-control>.
29. Dan DeCook, "Innovation, National Defense Strategy, the future: CSAF at Air Force Association Air Warfare Symposium," Secretary of the Air Force Public Affairs, February, 2018, <https://www.af.mil/News/Article-Display/Article/1449095/innovation-national-defense-strategy-the-future-csaf-at-air-force-association-a/>.
30. Department of the Army, *The US Army in Multi-Domain Operations: 2028*. TRADOC Pamphlet 525-3-1. Fort Eustis, Virginia, December 2018.
31. John Arquilla, et. al., *Russian Strategic Intentions*, Department of Defense, Joint Chief of Staff, May, 2019, <https://nsite-am.com/social/wp-content/uploads/2019/05/SMA-TRADOC-Russian-Strategic-Intentions-White-Paper-PDF-1.pdf>.
32. "Department of Defense Press Briefing by Secretary Esper and General Milley." U.S. DEPARTMENT OF DEFENSE, December 20, 2019, [www.defense.gov/Newsroom/Transcripts/-Transcript/Article/2045725/departement-of-defense-press-briefing-by-secretary-esper-and-general-milley-in-t/](http://www.defense.gov/Newsroom/Transcripts/-Transcript/Article/2045725/departement-of-defense-press-briefing-by-secretary-esper-and-general-milley-in-t/).
33. Herbert Lin, "The Existential Threat from Cyber-Enabled Information Warfare," *Bulletin of the Atomic Scientists* 75, no. 4 (2019): 187–96, <https://doi.org/10.1080/00963402.2019.1629574>.
34. Dina Temple-Raston, "How The U.S. Hacked ISIS." NPR. National Public Radio, September 26, 2019, <https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>.
35. Air Force Space Command, "The Future of Space 2060 and Implications for U.S. Strategy: Report on the Space Futures Workshop," 2019.
36. Nathan Strout and Aaron Mehta, "Russia Conducted Anti-Satellite Missile Test, Says US Space Command." C4ISR-NET. C4ISRNET, April 15, 2020, <https://www.c4isrnet.com/battlefield-tech/space/2020/04/15/russia-conducted-anti-satellite-missile-test-says-us-space-command>.
37. Travis Fedschun and Lucas Tomlinson, "Iran's Military Satellite a 'Tumbling Webcam in Space,' Space Force Commander Says." Fox News. FOX News Network, April 26, 2020, <https://www.foxnews.com/world/iran-military-satellite-us-space-force-commander-tumbling-webcam>.



# Countering Disinformation: Are We Our Own Worst Enemy?

---

Colonel (USA) Michael Jackson  
Paul Lieber, Ph.D.

## INTRODUCTION

In his 2019 book, *Information Wars: How We Lost the Global Battle Against Disinformation and What We Can Do About it*, Richard Stengel detailed the Department of State's (DoS) struggles in this burgeoning space. Stengel leaves the reader with a view of the United States Government (USG), where individual departments and agencies resist collaboration and tackle disinformation as individual departments and agencies. The result is a poorly integrated effort with limited awareness of parallel activities, significant challenges to cross-department and inter-agency collaboration, and the inability to evaluate and describe success or failure. Rather than accept Stengel's description as the only way the USG can function, this article posits counterpoints derived from direct involvement with multiple USG departments and agencies during both the Obama and Trump administrations. The counterargument is an understanding of cross-governmental authorities combined with collaborative implementation leads to greater success in combating disinformation.

To begin, Stengel's primary thesis is that, by design, democracies are naturally inadequate at countering disinformation. Inherent territorialism within a democracy is a critical weakness Stengel experienced, and is at the core of his criticism. In contrast, we propose that talent, initiative, innovative spirit, less centralized control, and ability are the real foundations of democracy and can, therefore, be collectively leveraged to both overcome territorialism and effectively counter disinformation. The greatest challenge lies in maximizing and synchronizing these strengths.

Stengel describes a widespread territorial mentality within and between USG departments and agencies. We acknowledge this mindset exists and stifles potentially successful ideas and efforts that require USG elements to work in partnership. In contrast with Stengel, our experience suggests this territorial mentality is something the USG can

*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 Michael J. Jackson** is Chief for Plans, Policy, and Partnerships at the Cyber National Mission Force. He was previously the Senior Army Fellow at the Council on Foreign Relations. COL Jackson has served as Chief for Information Operations and Special Activities at the Brigade, Division, Theater Special Operations Command, NATO Operational, and Global Combatant Command. He is an Information Operations officer with extensive experience integrating information related capabilities across the Department of Defense, within the whole of the United States Government, with NATO Allies and with partner nations. Assignments include United States European Command, Special Operations Command Europe, NATO, 1st Armored Division, 1st Infantry Division, and 2nd Infantry Division. Overseas assignments include Korea, Germany, Portugal, Iraq, Afghanistan, Jordan, and Kosovo. He earned a BA from The Ohio University, an MS from Naval Postgraduate School, and a MMAS from the College of International Security Affairs at the National Defense University.

overcome. The solution? (1) Link executive leadership and action officers across departments and agencies, (2) explain the intent to work together, (3) understand existing efforts rather than creating new ones, (4) create an understanding of departmental and agency authorities and capabilities, (5) appreciate permissions to apply authorities, (6) reduce the emphasis on differences and credit for successes. The crux of intergovernmental territorialism lies in a basic discussion of authorities absent a clear understanding of permissions. To this end, a mentor once told me: *amateurs* talk about **authorities**; *professionals* talk in terms of **authorities and permissions**.

Second, Stengel only served for two years as the Under Secretary of State for Public Diplomacy and was another example of the rapid rotation of key individuals throughout government. This rotation cycle occurs not only at the political appointee level but also at the executive and action officer ranks. The outside perspective brought by political appointees is essential in a functional government, and regular rotations will and should continue. However, this, combined with the rapid rotation of public servants at all levels, starves organizations of institutional knowledge and inhibits the development of coherent initiatives and the implementation of consistent policy. Furthermore, rapid rotation prevents the creation and sustainment of networks of professionals who understand cross-governmental authorities and permissions and who have the experience of cooperatively implementing them.

To achieve successful coordination in the disinformation war, USG should revisit perspectives from the administration of President Dwight Eisenhower, including his National Security Advisor Robert Cutler. Eisenhower was known for collaboration, and if you “put the right smart people in a room, they could figure out the answer to any problem” (Thomas 2012). To get those people in the room, Cutler described his role as that of an ‘information broker’ (Burke 2009). This solution, which





**Dr. Paul Lieber** is COLSA Corporation's Chief Scientist (Data & Social Science), where he specializes in communication influence. A Board Member of the Information Professionals Association, he previously served as the Command Writer for two USSOCOM Commanders, likewise Strategic Communication Advisor to Special Operations Command-Australia. Within academic environs, Dr. Lieber was full-time Graduate faculty at Joint Special Operations University, Emerson College, University of South Carolina, and the University of Canberra, respectively. He holds a Ph.D. in Mass Communication and Public Affairs and a Masters of Mass Communication from Louisiana State University, and a B.S. in Broadcast Journalism from Syracuse University.

is the antithesis to Stengel's argument, moved the Eisenhower administration away from territorialism and into a team mindset, which was based on a foundation of partnership.

### **EUCOM, RUSSIAN DISINFORMATION, AND THE 'RUSSIA INFLUENCE GROUP (RIG)'**

In late 2015 and following Russia's intervention in Ukraine, the USG was concerned with additional Russian interference in other former Soviet states. Specifically, the USG was troubled by the advanced levels of Russian disinformation and misinformation which were aimed at European partners and allies. Countering Russian disinformation outside the continental US required a whole-of-government resource synchronization to support DoS and individual country teams. The U.S. European Command (EUCOM)/DoS co-led Russia Information Group (RIG) was born from a need to understand and integrate USG efforts to defeat an increasingly robust Russian campaign of disinformation and misinformation, one intended to undermine the US relationships with partners and allies. The name was later changed to the Russia Influence Group (RIG) to enable a broader focus. It must be noted here, the Russia Influence Group (RIG) described here is different than the Twitter-based Russia Influence Group described by Stengel in his book. The somewhat parallel evolution and lifecycle of the two groups is an excellent example where awareness and interagency collaboration could have and should have taken place but did not.

Stengel's premise that democracies are inept at countering disinformation is not entirely off base. First, freedom of speech is a great US strength and a fundamental principle, but it possesses an inherent vulnerability. Adversaries regularly exploit US freedom of speech protections by inserting protected but untruthful claims into its information environment. Second, when integrating across the US interagency, understanding departmental culture and perspectives are critical as they are

frequently at odds. Differences in culture and perspective often feed interagency territorialism. DoS and the Country Teams, for instance, naturally focused heavily on individual countries. EUCOM and the Department of Defense (DoD) view the world as regions. For EUCOM, this includes over fifty countries with multiple sub-regions where defense requires a multi-state and collective effort. Bridging the DoS and DoD/EUCOM gap to create a more collective perspective was a challenging, but essential task for the RIG.

Four years later—in March 2019—EUCOM’s Commander (General Curtis Scaparrotti) described to Congress his approach to integrating EUCOM’s counter-disinformation activities with the rest of USG (Scaparrotti 2019). The partner approach was bifurcated into two levels of integration. The first was a monthly EUCOM / DoS, co-chaired meeting at the senior action officer level. The second was a bi-annual EUCOM / DoS Senior Leader Steering Board (SLSB) to guide action officers on the whole-of-government plans and emerging initiatives.

The aforementioned RIG (now a mature entity) would present integrated plans and activities to the steering board along lines of effort, including messaging, diplomatic engagement, energy-related issues, finance, and judicial-related issues, and support to the North Atlantic Treaty Organization (NATO). In many cases, Ambassadors or Deputy Chiefs of Mission returned to Washington, D.C., to attend the SLSB to brief or show support for the plans. Participation in the SLSB was voluntary, but the implementation of plans required consensus. Worth noting is this integration initiative would not usurp existing interagency process led by the National Security Council (NSC) and the National Security Staff (NSS). Instead, the process supported bottom-up development in response to guidance provided by said NSC and NSS.

A separate but critical supporting effort to the EUCOM/DoS RIG partnership was the annual Europe Chief of Mission Conference. This effort assembled Chiefs of Mission from across the EUCOM area of operations, leadership from the Department of State European and Eurasia Bureau, and EUCOM Staff (e.g., military personnel, and the EUCOM J9 Interagency Partnership Division consisting of senior liaisons from across USG). The Chiefs of Mission conference empowered DoS, EUCOM, and Chiefs of Mission to share insights on current and burgeoning efforts, to include the RIG. The result was broader awareness, integration, and inclusion.

The final supporting effort was the EUCOM led Russia Strategic Initiative (RSI), which General Scaparrotti described in his 2017 testimony to the House Committee on Armed Services (Scaparrotti 2017). The RSI focused on DoD integration to balance deterrence and escalation. All three efforts (RIG, Chief of Mission Conference, and the RSI) included the DoS and the broader interagency and exemplified EUCOM’s pursuit of a whole-of-government partnered approach in Europe.

For the RIG to be successful, communication was paramount, and dedicated liaisons located in the National Capital Region (NCR) augmenting support from DoD and DoS leadership were essential to ensuring communication occurred and momentum was maintained. A critical liaison built and maintained relationships with key USG departments and agencies. Another

significant liaison worked in the DoS Europe Eurasia Bureau (DoS EUR) handling RIG scheduling and coordination. Importantly, the DoS EUR liaison communicated and translated between DoD and DoS speak. Liaisons ensured visiting senior EUCOM leadership reinforced existing and substantive conversations and aided in strengthening support. Liaisons also ensured plans and concepts submitted to the SLSB were fully coordinated and ready for senior leader approval or guidance. This was a stark contrast to the typical wave top senior leader engagements and these liaisons significantly reinforced partnerships.

General Scaparrotti consistently emphasized that while EUCOM would appropriately lead and shape RIG efforts, too much defense influence and oversight would be counterproductive. His interaction with the US interagency process repeatedly reinforced the principle that great leaders must effectively balance between leading and following. Great leaders are also great partners. Contrary to Stengel's territorial experience, when the RIG collectively presented integrated proposals to USG leaders, one of two outcomes occurred. Either decision-makers emphatically supported implementation, or they worked out differences face-to-face, reducing potential weeks or months of staff coordination to minutes. Ultimately, participating departments and agencies viewed ongoing parallel efforts as complementary to their own goals and objectives.

Summarizing fundamentals learned from the past and reinforced by the RIG:

1. The singular problem, countering Russian misinformation and disinformation meant to undermine US credibility in Europe, required focused and enhanced collaboration. The RIG recognized and embraced this.
2. A two-tiered structure creates organizational commitment of staff and resources in addition to executive leadership obligation to supervise execution. For the RIG, this included: monthly communication and close collaboration between action officers and bi-annual forums for executive decision-makers to jointly approve or supply guidance to action officers.
3. Liaisons grow networks and reach. RIG liaisons mitigated the cost of participation by member organizations, enabled open and transparent communications, and supported face-to-face relationships.
4. Success requires an understanding of and respect for participating members. For the RIG, this meant maintaining the highest familiarity with partner authorities, and employing institutional liaisons (point 3) to bridge organizations and cultural differences.
5. Informal is often a good path. The informal nature of the RIG where cross-departmental and agency network participation was voluntary, reduced tension and pressure to participate.
6. Consider a partnership agreement upfront. This agreement was used by RIG members to develop plans through consensus, share credit, and create a forum for open discussion.

## HOW TO COLLABORATE ON COLLABORATING

Collaboration is where problems and opportunity lie. Democracies can be exceedingly effective at countering disinformation. Effectiveness requires the time to understand and leverage the authorities and responsibilities of each department and agency across USG. An effective approach also requires that organizations understand and work with partners and allies, is inclusive of industry, non-profits, academia, and encourages innovation. There are three steps the USG can take right now to improve collaboration to counter adversary disinformation:

1. Train individuals how to work across the interagency.
2. Learn to develop a strategy from the bottom up. These efforts should not replace the interagency process or documents, but rather complement existing strategies and practice.
3. Maximize non-USG entities in determining the assessment of best practices and baselines.

Addressing the first point requires an investment in the education of individuals serving in government. These individuals must have a clear understanding of their department or agency, their capabilities, and their organization's authorities. Second, they require an additional understanding of how to integrate with sister departments' and agencies' capabilities and authorities. In DoD, each service possesses robust professional education systems. Additionally, gateway schools and professional development exist for promotion at each critical step in an individual's career. However, none of these schools adequately prepare individuals to effectively interact and leverage the interagency environment.

To the second point, USG must also re-consider career progression and job rotation in the military and across government. At too many departments and agencies, individuals serve only two to three years in a job before rotating to a more senior position. The focus is on the promotion of generalists rather than the creation of skilled career practitioners. Frequently moving individuals also creates a lack of continuity between policy and strategy. Tackling disinformation problems requires those most skilled at employing and integrating solutions. Relatedly, across much of USG, information professionals are respected, but collectively, are not seen as competitive for promotion to the most senior and executive ranks. Management of strategic campaigns and narratives require the skill, experience, knowledge, and intuition of an executive campaign manager.

Interagency groups need to supply better, broader, and more inclusive solutions to the existing interagency process. That being said, creating more groups is not the answer. An informed, networked approach will yield more focused and fewer ad-hoc organizations; staff will naturally realize others are working on the exact same problem.

Lastly and addressing the third point, the USG must think beyond industry as a means to employ contractors to fill gaps in operational needs. Industry is adept at understanding marketing, data, and social science principles, evaluating long-term trends in the environment,

and maintaining technology to quickly identify patterns in disinformation. Cooperative partnership with industry should include informal and professional relationships (i.e., advertising executives, cybersecurity officers, communications professionals, and others from the top and most innovative firms) to better analyze the disinformation problem and understand emerging solutions.

This inclusive approach also requires partnerships with think tanks, non-profits, and 501(c)(3)-type organizations that exist solely to advise and assist government in analyzing and developing innovative disinformation solutions that affect both government and industry.

Importantly, even the arguably successful RIG never conquered disinformation assessment and evaluation, specifically developing a proper baseline understanding of the current information environment to then determine success. There are still extreme barriers and outright refusals across the USG to share internal information measurement methods or to consider external assessment and evaluation. There is also a reticence to leveraging marketing and other industry skill and expertise. Collaboration in these areas remains a significant obstacle to overcome.

## **NURTURING FROM WITHIN TO GROW FROM BEYOND**

The root of territorialism lies in cultural and institutional norms, most of all in talent management. To better manage career professionals and develop talent and utilizing input from industry, the Army created the Talent Management Task Force and developed the Assignment Interactive Module (AIM). Though not completely perfect, AIM is a significant improvement over its highly decentralized predecessor. AIM demonstrates the Army's commitment to develop true professionals and make a concerted effort to deliberately match expertise to the job. Moreover, AIM enables officers to work outside of their career field, expanding their professional skills and knowledge in tandem. The Army's implementation of brevet promotions and providing officers an ability to delay participation in key selection boards without prejudice offers flexibility. While it is nothing new for officers to serve in a billet above their current rank, the newly implemented brevet promotion policy promotes the individual to the required rank, and the individual receives pay and benefits of the higher rank for the period they hold a billet senior to their current rank. Likewise, providing officers the opportunity to delay a promotion or selection board to remain in key developmental billet an additional year is significant. This flexibility yields increased influence in Army career progression by one's supervising officers, career managers, and leadership. This also means officers can stay in critical jobs longer and gain essential experience that will significantly benefit the USG. There is no doubt other USG departments and agencies are pursuing similar talent management improvements, with best practices to learn and share.

The DoD has, for decades, required significant institutional commitment and investment in education and professional development. The Goldwater-Nichols Act, intended to fix challenges

to Joint operations such as the failure of Desert One in April 1980, recreated DoD's education, and assignment process. This, however, was a military solution that did not realistically extend to the interagency. Also, changes to education and promotion resulting from Goldwater-Nichols did not significantly affect officers below the rank of Colonel. To this day, officers lacking enough experience in a Joint environment are easily identifiable. In tandem, a whole-of-government solution must be developed to expose action officers and public servants to each other sooner. Sincere consideration of a Goldwater-Nichols Act for the interagency is therefore critically needed.

The final, persistent talent-centric problem remains collaboration and partnership beyond the USG. The rule, 'do what you are good at, and do not try to be something you are not,' still applies. Government agency professional development systems deliberately cultivate generalists, leaders, and decision-makers to manage organizations and produce and implement policy. As such, critical capabilities remain where USG is simply incapable of maturing techniques and maintaining the talent not just to be competitive, but to win.

Thus, and in some cases, contracting from traditional government contractors remains a solution. In others, including operations in the information environment, infusing current industry experience beyond the usual government-centric talent pool is truly needed. This importantly includes building relationships with industry providers to identify future needs. For example, relationships with industry leaders in marketing and evaluation expose action officers to ideas, concepts, and techniques at the leading edge of industry. Industry cybersecurity experts possess a perspective vastly different than cyber professionals within the government. Increasing industry fellowships with junior officers, captains, and majors, would expose individuals to leading technology and enable them to bring their experiences and relationships back to DoD.

## **CONCLUSION**

The COVID-19 crisis presents a significant opportunity for government and industry-wide collaboration in the information space and beyond. The crisis finds organizations like Thompson Reuters working with Facebook to identify and explain misinformation and disinformation throughout social media. The DoS Global Engagement Center's (GEC) Technology Engagement Team is now leading USG toward finding, developing, and evaluating capabilities available from industry. The National Security Innovation Network (NSIN) is yet another bright spot during COVID-19, a resource that conveys significant USG collaboration and partnership potential. Multiple other departments and agencies across the USG are looking at COVID-19 as a threat with varying levels of integration being the solution.

A crisis also often leads to the creation of new organizations and working groups who are focused only on a single problem. The COVID-19 crisis—like its highest-profile counterparts—transcend every societal boundary and organizational proclivity to focus on 'the current problem.' With disinformation accompanying the crisis, there are two choices: (1) to either view

adversary sponsored COVID-19 disinformation and misinformation as a separate information campaign, or (2) to realize that COVID-19 disinformation and misinformation are opportunistic adaptations by adversaries who aim to reinforce existing narratives. The COVID-19 disinformation is clearly an opportunistic adaptation and provides a common motivation across the USG to rapidly strengthen and integrate existing efforts. The opportunity to leverage this crisis to fundamentally improve the way we collaborate to counter disinformation and misinformation is one we cannot afford to miss.

As the ‘solution’ noted above, far from being incapable of countering disinformation, the decentralized collaboration of the USG’s amalgamation of authorities, capabilities, and the professionalism and initiative of dedicated public servants is more than capable of countering the adversary’s centralized and focused approach. Overcoming USG territorialism is the most significant roadblock, but the RIG proved that this is anything but insurmountable. Developing professionals across the interagency to understand cross-departmental capabilities, authorities, and permissions are feasible. Creating networks of action officers and executive leadership across the interagency are attainable. It is essential that executive leadership and actions officers adopt an attitude of partnership.

In closing, and to both acknowledge and counter Stengel; The US must become comfortable owning its narrative and through collaboration across and external to the USG. When founded on collaborative partnership, without a doubt, democracies are exceedingly more capable of countering disinformation.♥

## **RECOGNITION**

Throughout this article, we reinforced the importance of an inclusive partner approach, and with it leveraging a community of experts and professionals. To that end, it is essential to recognize the leaders, practitioners, and partners essential to making the RIG successful. These individuals included: General (R) Curtis Scaparrotti, Mr. Wess Mitchell, Deputy Assistant Secretary of Defense Laura Cooper, General Timothy Ray, Lieutenant General Stephen Twitty, Lieutenant General Patrick White, Major General (R) Skip Davis, Major General David (Oscar) Meyer, Ambassador Susan Elliott, Ambassador Philip Reeker, Ambassador Dennis Hearne, Ambassador Eric Rubin, Ambassador Kyle Scott, Mr. Ben Ziff, Me. Lea Gabriel, Ms. Sharon Hudson-Dean, Ms. Yaryna Ferencevych, Ms. Meghan Gregonis, Colonel Sonny Legget, Colonel (R) Josh Burgess, Colonel Paul Matier, Colonel (R) Bo Clayton, Colonel Vic Garcia, Colonel Rob Kjelden, Colonel (R) Bryan Sparling, Colonel Brian Mellen, Lieutenant Colonel Dan Welsh, Mr. Patrick Fetterman, Mr. Austin Branch, Mr. Jeff Trimble, Mr. Gary Thatcher, Mr. Daniel Kimmage, Ms. Adele Ruppe, Mr. Chris Dunnnett, Ms. Alicia Romano, Ms. Tonia Weik, Ms. Marta Churella, Mr. Oscar DeSoto, Mr. George Franco, Ms. Patricia Watts, Mr. Hunter Treseder, Ms. Lauren Protentis, Mr. Al Bal, Ms. Wendy Bartley, Ms. Christina Madrid, Ms. Alden Burley, Ms. Rohina Phadnis. The excellence of these individuals and other not named resides in those after them who follow their examples.

## NOTES

- John P. Burke, 2009, *Honest Broker?: The National Security Advisor and Presidential Decision Making*. Texas A&M University Press.
- Graeme P. Herd, 2019, "Executive Summary: Understanding Russian Strategic Behavior," no. 10: 4.
- Isaac Porsche, Christopher Paul, Chad Serena, Colin Clarke, Erin-Elizabeth Johnson, Drew Herrick, 2017, "Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below," RAND.
- "Scaparrotti\_03-05-19.Pdf," accessed March 24, 2020, [https://www.armed-services.senate.gov/imo/media/doc/Scaparrotti\\_03-05-19.pdf](https://www.armed-services.senate.gov/imo/media/doc/Scaparrotti_03-05-19.pdf).
- "Scaparrotti\_03-28-17.Pdf," accessed April 13, 2020, <https://docs.house.gov/meetings/AS/AS00/20170328/105780/HHRG-115-AS00-Wstate-ScaparrottiC-20170328.pdf>.
- Richard Stengel, 2019, *Information Wars: How We Lost the Global Battle against Disinformation & What We Can Do about It*. First edition. New York: Atlantic Monthly Press.
- Evan Thomas, 2012, *Ike's Bluff: President Eisenhower's Secret Battle to Save the World*. Vol. 1. New York: Little, Brown and Co.







# THE CYBER DEFENSE REVIEW

◆ PROFESSIONAL COMMENTARY ◆



# Building the Army's Artificial Intelligence Workforce

---

Major Nathaniel D. Bastian, Ph.D.

Artificial intelligence (AI) is a set of algorithmic tools and technologies that enable machines to perform tasks that normally require human intelligence—such as perceiving the world, learning from experience, reasoning through information, representing knowledge, acting, and adapting.<sup>[1]</sup> Given the multitude of rapid technological advancements in AI, computing, big data analytics and autonomy, the 2018 National Defense Strategy (NDS) emphasized the importance of leveraging the “very technologies that ensure we will be able to fight and win the wars of the future.”<sup>[2]</sup> The 2018 NDS flags ways to modernize key capabilities in “address[ing] the scope and pace of our competitors’ and adversaries’ ambitions and capabilities,”<sup>[3]</sup> and the need to “invest broadly in military application of autonomy, AI, and machine learning, including rapid application of commercial breakthroughs, to gain competitive military advantages.”<sup>[4]</sup>

Introducing AI capabilities into the military will impact virtually all Army warfighting functions, including: mission command (e.g., battlefield virtual assistant for command and control), movement and maneuver (e.g., self-driving tanks, helicopters, and other vehicles), fires (e.g., autonomous weapon systems and AI-enabled targeting), sustainment (e.g., predictive maintenance and logistics), protection (e.g., anomaly detection to protect critical infrastructures), intelligence (e.g., AI-based information collection, data fusion and analysis), and special operations. Creating a robust AI workforce challenges the Army’s organizational capacity to best leverage and grow AI talent. At a minimum, changes are needed to ensure that resources will be available to complement the AI workforce changes, but that they will be available in a way that will better support the Army’s operating forces.

*This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply. The views expressed in this work are those of the author and do not reflect the official policy or position of the United States Army, the Department of Defense, or the United States Government.*



**MAJ Nathaniel D. Bastian, Ph.D.** is an FA49 (Operations Research / Systems Analysis) Officer in the U.S. Army. He currently serves as the Chief Artificial Intelligence Architect at the Department of Defense Joint Artificial Intelligence Center (JAIC), where he provides strategic direction and technical leadership for artificial intelligence (AI) activities, to include technical advisement, expertise and oversight of data science and AI engineering functions across the JAIC. He also serves as Senior Research Scientist and Adjunct Assistant Professor at the Army Cyber Institute at West Point, researching in the areas of autonomous cyber decision-support and AI system assurance. He holds a Ph.D. degree in Industrial Engineering and Operations Research from Penn State University, M.Eng. degree in Industrial Engineering from Penn State, M.S. degree in Econometrics and Operations Research from Maastricht University, and B.S. degree in Engineering Management (Electrical Engineering) with Honors from the U.S. Military Academy at West Point.

In response to the 2018 NDS, the Office of the Department of Defense (DoD) Chief Information Officer (CIO) established the Joint Artificial Intelligence Center (JAIC) with the “overarching goal of accelerating the delivery of AI-enabled capabilities, scaling the Department-wide impact of AI, and synchronizing DoD AI activities to expand Joint Force advantages.”<sup>[5]</sup> To fulfill the DoD AI Strategy, JAIC’s main focus areas will be recruiting, training, promoting, and retaining a leading AI workforce.<sup>[6]</sup> To buttress JAIC’s efforts, the Army established the Army-AI Task Force (A-AI TF) under the U.S. Army Futures Command (AFC) to “rapidly integrate and synchronize AI activities across the Army.”<sup>[7]</sup> One key task is to “develop a talent management plan for the acquisition and retention of necessary skillsets to support Army machine learning and AI activities today and into the future.”<sup>[8]</sup> The U.S. Army Combat Capabilities Development Command (CCDC), formerly the U.S. Army Research, Development and Engineering Command (RDECOM) underscored this need for “AI-fluent scientists and engineers, and to establish opportunities for developing AI-fluency in the current workforce.”<sup>[9]</sup> Integrating AI into the Army means accommodating, growing, and maintaining the requisite skilled AI workforce. Similar to the distinctive way that network and cyber expertise have evolved, AI will require personnel with specialized talents. To create and grow the Army’s AI workforce will require key changes to the existing force structure and AI career management.


For Army officers in all applicable components (COMPO), an existing career management field (CMF), such as Functional Area 49 (FA49) Operations Research/Systems Analysis (ORSA), will require change. While the FA49 officer “introduces quantitative and qualitative analysis to the military’s decision-making processes by developing and applying probability models, statistical inference, simulations, optimization

and economic models,”<sup>[10]</sup> FA49 officers will have an unprecedented opportunity to refine the delivery of their tradecraft. In particular, the FA49 Proponent Office seeks FA49 officers who will “take advantage of the cloud, the open source environment, big data, and algorithms.”<sup>[11]</sup> Over the past few years, the FA49 Proponent Office has heavily invested in providing opportunities to integrate data science and more advanced ORSA skills into the FA49 training pipeline via graduate schooling, continuing education, training with industry, and professional military education. As a result, the bench of FA49 officers equipped with the latest data science skills has grown considerably. In order to certify, track and manage the Army’s FA49 officers with data science qualifications, the Headquarters, Department of the Army (HQDA) G-1 in conjunction with the FA49 Proponent Office established the Personnel Development Skill Identifier (PDSI) R1J for Data Scientist, which certifies that the FA49 officer has met specific graduate degree (master’s or doctorate) requirements and has requisite experience working with distributed computing platforms along with one or more programming languages (R, Python, etc.), structured query language (SQL), and Linux command-line interface commands.<sup>[12]</sup>

While the supply of data science-trained officers has increased, so too has the demand. More and more organizations across the Joint Force seek FA49 officers to lead data science efforts. Indeed, along with the creation of JAIC and A-AI TF organizations, and publication of the DoD AI Strategy, demand for FA49 officers armed with AI skills has grown exponentially. In terms of AI talent, the FA49 Proponent Office wants FA49 officers to “become the experts in not just understanding how the algorithms work, but how to put together the team to make the algorithms work properly.”<sup>[13]</sup> While several FA49 officers have the necessary education, training and technical leadership experience to serve as Army AI experts and leaders, the bench remains relatively small given the high demand across the Joint Force. Further, AI-savvy FA49 officers currently are not managed in a distinct military occupational specialty (MOS); the FA49 CMF has only one managed MOS, 49A, for a generalist ORSA. Typically, the 49A MOS does not require FA49 officers to possess the expert mathematical, computational, cognitive, and software development skills such as machine learning engineering, evolutionary computation algorithm design, and human systems integration, that are necessary for the AI tradecraft. This dearth of managed AI talent and respective force structure requires a fix to this obvious DoD and Army-wide capability gap.

Creating and definitizing a managed 49B MOS for an Army AI career specialty within the FA49 CMF would help enable and enhance the Army’s ability to recruit, train, promote and retain AI personnel required by the Joint Force. This would mean major changes to the Army’s FA49 force structure, and to AI personnel policies and career management, AI education/training, and AI workforce development. Moreover, the timely creation of this managed AI career specialty within the FA49 CMF would help move the Army in the right direction for building a leading AI workforce. The creation and management of the 49B MOS career

specialty and resulting force structure would jump start and help sustain recruiting, training, promoting, and retaining talented FA49 officers who can lead the design, development, testing, evaluation, assessment, and implementation of AI tools and technologies across the Army's operating and generating forces. AI talent management within the FA49 CMF requires effective processes and procedures, and is essential if we are to optimize AI capabilities as an integral part of the Army's warfighting functions.

This proposed solution helps build, grow, and manage a talented and leading Army AI workforce needed to operationalize AI capabilities into the DoD to "fight and win the wars of the future."<sup>[14]</sup> Further, this solution directly supports the recommendations of the National Security Commission on Artificial Intelligence (NSCAI) for recruiting, training and retaining a world-class, AI-ready workforce in accordance with its recently established common AI Workforce Model developed in partnership with the Defense Innovation Board and the JAIC to guide DoD AI workforce needs.<sup>[15]</sup>



## NOTES

1. Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity* (Washington DC, 2018), 5.
2. Department of Defense, *Summary of the 2018 National Defense Strategy (NDS) of the United States of America: Sharpening the American Military's Competitive Edge* (Washington DC, 2018), 3.
3. *Ibid.*, 6.
4. *Ibid.*, 7.
5. Patrick M. Shanahan, Acting Secretary of Defense, *Establishment of the Joint Artificial Intelligence Center* (Washington DC, 2018), 1.
6. DoD AI Strategy, 14.
7. Mark T. Esper, Secretary of the Army, *Army Directive 2018-18 (Army Artificial Intelligence Task Force in Support of the Department of Defense Joint Artificial Intelligence Center)* (Washington DC, 2018), 1.
8. *Ibid.*, 3.
9. U.S. Army Research, Development and Engineering Command. *RDECOM Artificial Intelligence Study* (Aberdeen Proving Ground MD, 2018), 1.
10. Headquarters, Department of the Army, *Department of the Army Pamphlet 600-3. Chapter 31* (Washington DC, 2014), 310.
11. MG John G. Ferrari, FA49 Executive Agent, *FA49 Proponent Update* (Washington DC, 2018), 5.
12. Headquarters, Department of the Army, *Department of the Army Pamphlet 611-21. Chapter 1, Table 1-2 (PDSI)* (Washington DC, 2018), Table 1-2.
13. MG John G. Ferrari, 6.
14. Department of Defense, *2018 National Defense Strategy*, 3.
15. United States of America, National Security Commission on Artificial Intelligence, *Interim Report for Congress* (Washington DC, 2019), 35, 61-65.



# Truth Dies First: Storyweapons on the InfoOps Battlefield

---

Renny Gleeson

Storyweapons are adversarial narratives that use algorithms, automation, codespaces, and data to hijack decision-making, and the stories of who we are, what we believe and why it matters. They leverage vulnerabilities and weaknesses against people and populations; they subvert freewill to bend actions to self-sabotage. Storyweapons exploit attack vectors across our new mixed reality of code and cognition, and they move the frontlines into the minds and software connected to any strategic objective. Defending the US against storyweapons requires a reconsideration of battlefields, operational models, and threat actors.

Storyweapons are a new class of threat, fielded by new threat actors in non-traditional domains across the new landscape of Codespace. A military “prepared to fight the last war” risks missing the one raging now: storyweapons are evolving, mutating, and redefining how we wage war and peace in real-time. To “defend the United States against all enemies” means defeating foreign and domestic adversaries who use storyweapons to attack our democracy, our institutions, and our people. They are doing it right here, right now, and from every screen, weaponizing the information environments and the connected spaces in which we live. “The future of disinformation is domestic,” noted Alex Stamos, Facebook’s former security chief<sup>[1]</sup>.

To unpack storyweapons, we first must know why the “story” is important.

Maybe you know the story about the astronaut’s pen. It goes something like this: Back in the sixties, American astronauts needed something to write with in space, so NASA put in years of research and spent millions of tax dollars to develop a pen that could work up there. A masterpiece of engineering, it had pressurized ink and a carbide-ball tip so it could write upside down and in zero G. The Soviets, well they had the same problem. They gave their cosmonauts pencils. It’s a great story, but it’s not true.



**Renny Gleeson** works at Wieden+Kennedy (W+K), the world's largest independent creative ad agency. W+K handles some of the world's most well-known brands, and was named "Agency of the Year" the last three consecutive years. Renny joined W+K in 2007 to lead interactive strategy, and served on the global management team. In addition to direct client work, he co-founded and led W+K's tech/business accelerator and now leads W+K BIG, the W+K Business and Innovation Group focused on business and brand experience transformation. An industry leader and TED speaker, he writes, studies, and speaks on persuasive technologies and the ways they shape and are shaped by human behavior. The views expressed here are his own.

Truth seldom matters when it comes to stories - what matters is how they feel. Just look at our political situation. The truth about the pen is that a private company developed the pen at its own expense. As for pencils, they introduce flammable material into the cabin and can generate broken lead, a threat to astronauts and their equipment. The truth is that once the pen was invented, the Soviets ordered them from the same company.<sup>[2]</sup> But "truth alone," as Carl von Clausewitz wrote, "is but a weak motive of action with men...the strongest impulse to action [is] through...feelings"<sup>[3]</sup>: the 'astronaut pen' is a story that feels *true enough* - it resonates, and stories that resonate, propagate. Along the way, our most deeply felt stories become foundational to our individual and collective identity. At that level, they become impervious to truth. We pay no attention to facts that put those stories at risk; from a sensory standpoint, we literally do not see them. As Daniel Kahneman wrote in *Thinking Fast and Slow*, "The confidence that individuals have in their beliefs depends mostly on the quality of the story they can tell about what they see, even if they see little."<sup>[4]</sup> Stories—especially the deep stories that exist beyond words and rationality—do not describe reality; they are the filters through which we create it.

Our stories are more vulnerable than we know: our cognitive systems are hackable by everyone, from kids' birthday party magicians to infowar adversaries. We do not see the flaws in those systems because they are features of the systems. Storyweapons leverage the infrastructure of perception to misguide, misdirect, and manipulate.

We interpolate "meaning" not from *facts* but from estimations of relationships between them. Interpolation enables us to build stories from intuitive leaps, using extremely limited data, but the trajectory of those leaps (and where we land) is influenced by our biases, heuristics, hacks, and filters operating below

conscious cognition. Sensory information is filtered first through the amygdala (our “reptile-brain” of “fight-or-flight”) then through the mid-brain limbic system (our emotional/feeling brain) before reaching the frontal lobe (our rational/thinking brain). By biological design, outrage, fear, and the unfair light up these lower regions, grab the spotlight of our attention and short-circuit rational thought. This functional truth renders us vulnerable to adversarial attacks through media and software-mediated platforms. It also makes us vulnerable to attention hijacking by the platforms themselves, who monetize our attention in service to advertisers and third parties. They compete to grow attention share and revenue, and that competition becomes a race down the brain stem: research shows that joy moves fast over social networks, “but nothing is speedier than rage.”<sup>[5]</sup> The ruthless economic imperative behind the zero-sum wars for attention has fueled the rise of outrage as a business model in the places we connect with who and what we love.

Knowing what makes and motivates someone provides an instruction manual for actuation. A study by Gloria Mark at UC Irvine<sup>[6]</sup> showed one could predict the “big five personality traits” —Openness, Conscientiousness, Agreeableness, Extraversion, and Neuroticism—to 80% accuracy based on click streams, interactions, and behavior. This is precisely the data Cambridge Analytica leveraged to achieve their clients’ goals. What we *do* online is who we are, and we are online all the time: our digital signatures and data contrails lay bare our deep stories and our subconscious biases, filters, and desires. Adversarial Artificial Intelligence and Machine Learning systems that access our behavioral data can weaponize things about us we do not even know ourselves. Those adversaries are full-spectrum—one major US insurance company used its algorithms to predict how high insurance rates could be jacked up before a customer would switch to another provider; a 2019 U.N. report<sup>[7]</sup> suggested that with the advent of facial recognition software, eye-tracking and dynamic voice sentiment analysis, we might need to legally protect the right to dishonesty. When we touch software, or software touches us, we are known.

Software no longer sits safely behind the glass of our computer monitors or mobile devices; it permeates our environments, introduces new functionalities and vulnerabilities, and transforms decision-making, and the frameworks within which decision-making takes place to create new, symbiotic *decision spaces*.

Software, like gravity, has become a fundamental force of human experience—it can’t be talked about in a discrete domain, because it affects all domains. Our stories move through, shape, and are shaped by software; it has fused the physical (what you see), informational (what you capture/organize), and cognitive (sense-making, or CogSpace) domains to create the new world—and battlefield—of *Codespace*.

The interplay between CogSpace and CodeSpace is a continuum of heavily contested Information Environments. CodeSpace’s algorithmic “decisions” determine and reframe the

raw materials we use to sense-make in CogSpace; CogSpace’s narrative-influenced human “decisions” generate data that inform CodeSpace “learning,” dynamic reconfiguration and outcome-based optimization.

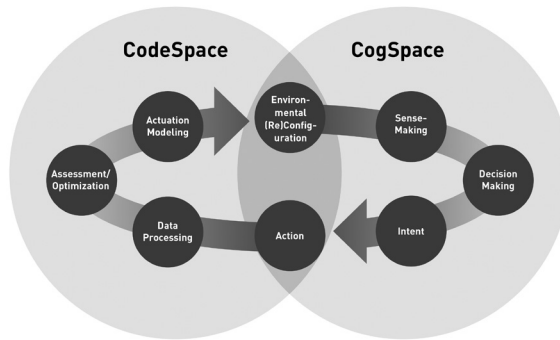


Figure 1: Storyweapon Threat Landscape

In these new decision spaces, we make conscious and unconscious decisions based on software, with software making decisions based on us. Our environment itself is alive, learning, aware. It has memory, biases, and opinions. Actors—private and state, foreign and domestic—fight for their agendas and our attention in these spaces; their actions and algorithms generate the raw materials of sense-making we use to build our stories of truth, identity and meaning.

Codespace was coined in 2014 by Kitchener and Dodge to describe what they called “life-as-software-mediated-experience”<sup>[8]</sup>. A typical airport demonstrates their premise: software is used to book your flight, integrate that flight into your calendar software, call a car to the airport, check you in, process and route your luggage; navigate you through security, determine your identity/threat level/processing path; tell you your gate, access public Wi-Fi or private “hotspots,” keep you entertained while you wait, dynamically alert you to departure and arrival time changes, enable plane access and status perks, and then fly the plane to your destination. An airport without code isn’t an airport—it’s a shed full of angry people surrounded by metal paperweights full of jet fuel. Airports are Codespaces.

Codespaces blur the lines between software, hardware, and experience; they will evolve to deliver customized video, audio, and haptic experiences. Google search results are already different for each user (based on historical searches and online behavior); soon real-world experiences will be, too: in the fall of 2020, some Detroit Metropolitan Airport travelers will experience custom visual beamformed airport signage (ala Minority Report) linked to their boarding pass, preferences, and physical position. Two travelers, looking at the same sign, will see different messages. “Dark marketing,” made notorious by the Cambridge Analytica revelations, is digitally targeted micro-persuasion, impossible to see as a whole, invisible to all but the targeted mind, vanishing once the emotional payload is delivered to the brainstem. Codespace enables this in the real world.

We will be alone together: two people looking at the same thing at the same time will sense different things. When lived experience is addressable, it becomes relative and vulnerable—and everything will be addressable. IPv6, the new Internet protocol being globally rolled out, has created enough new addresses to uniquely connect every atom on this earth to the Internet, with enough left over to connect 100+ more earths<sup>[9]</sup>. In self-optimizing addressable codespace, the truth becomes relative.

Storyweapons exploit all these technologies and more: the doctored video that tells us stories that reinforce our “illusory superiority”<sup>[10]</sup> will become augmented realities that amplify polarization; “beam-forming” will deliver micro-targeted visual, auditory, and haptic experiences in the real world, undetectable to anyone but the intended recipient; synthetic entities will be able to call, text or video chat with you, dynamically evolving their responses to your voice signature or facial expressions. Storyweapons will use a continually evolving tactical toolkit against people on the physical battlefield and use codespace to bring everything connected to combatants into the fight as well. War will not be fought “over there,” it will be fought in your mind, your home, your social connections, and in the court of public opinion.

Codespaces are battlefields that will dynamically reconfigure decision spaces and rewrite perception. By 2025, it is estimated that 5G will achieve 15% penetration globally and 74% in the US<sup>[11]</sup>; a functional promise of 5G is sub-1ms *latency*, the time it takes for your input through a software interface to generate an outcome. High latency is why the maps app on your phone tells you to take an exit after you’ve passed it on the freeway; low latency might win you the battle royale in Call of Duty’s Warzone. Biologically, neural processing is such that our perception of reality lags actual reality by about a tenth of a second<sup>[12]</sup>. Codespace operating with sub-1ms latency is a reality that can change in response to our feeling brain before our thinking brain consciously experiences it.

Three reasonable assumptions about Codespace operations include:

- 1. *Everything is compromised.*** Every interaction with Codespace generates, shares, and potentially leaks behavioral data. Hardware and chipset suppliers answer to their nations of origin (e.g., China’s National Intelligence Law). Social software experiences are powered by supercomputer arrays running algorithms that exploit our weaknesses and vulnerabilities to serve third-party agendas, learning, and self-optimizing at the speed of light. Finally, codespace is networked “systems of systems” with all the interoperability, incompatibility, integration and software updates and security patch headaches that implies. The Codespace we live in is neither safe, nor housetrained. Any software-mediated experience or enabling connection is an attack vector for storyweapons.
- 2. *Vulnerability is a feature, not a bug.*** More connections = more sensors = more data = more value. Connecting all those things—your printer, your coffeemaker, your thermostat—has to be easy or we would not buy them. According to security researchers

in 2017, having just five passwords would have allowed access to 10% of the world's estimated 8.4B Internet-connected objects whose users had not changed their original password<sup>[13]</sup>.

**3. Attack vectors multiply exponentially, not linearly.** Codespace environments are seldom single-author systems. Expect Frankenstein-ed systems of systems: a shit-sandwich of cascading dependencies and budget-restricted kluges running new and legacy hardware, multiple software configurations, and generations-old, unpatched security. These systems can be their own worst enemies even before adversaries compromise them.

Everyone and everything that touches software is effectively on the new Storyweapon battlefield; there is no “behind the lines.” All an adversary needs to secure “narrative” or “reflexive” control is enough data to tell the story you want to hear. And that story doesn't have to be true, it only must to be *true enough*.

The most effective marketing does not sell you a product; it sells you the story that the product tells about you, an emotional and aspirational story of who you'd be with that product in your life. We vote for the best stories with our attention. And if that story is compelling enough, if it feels true enough, it might break through the wall of 5-10,000 brand messages<sup>[14]</sup> and 12.5 hours of media we consume daily<sup>[15]</sup>. If we see in it something we want to believe about ourselves, we might splice elements of that story into our *deep story* DNA. Done at scale, you can sell product, move markets, shape opinion, and drive action.

You can't beat a “true enough” storyweapon with facts.

The only way you beat a story is with a better one.

To field a storyweapon tailored to its target, one needs data. One can steal data to build targeting profiles—38 Billion customer data files have been breached or hacked in the US alone since 2010<sup>[16]</sup>. You also can do what marketers do: buy it from the AdTech players fighting it out in the \$7 Trillion dollar attention industry. ChiefMartech's annual roundup lists 7,040+ marketing tech companies (up from 150 in 2011)<sup>[17]</sup>—for illustration purposes, consider just three: one is a data aggregator that claims to have dynamic, ongoing location data for 25% of the world's population; a second provides a mobile application that aggregates the data from 100 Billion data transactions by 1.4 Billion people across more than 7 Billion devices. At the CyCon U.S. conference in Washington DC in November of 2019, speaker Admiral (Ret.) Mike Rogers told attendees that China's government had amassed “2,500 data points per citizen”; four years prior, our third example, a US data brokerage subsequently acquired by an ad agency holding company bragged it had over 5000 data points per person<sup>[18]</sup>. When a single company on a roster of over 7,000 can make China's state surveillance look amateur, you must wonder about the rest. The sheer volume of legally and illegally available data makes it conceivably possible for any actor, foreign or domestic, to have already developed profiles for every potential “target of interest,” including everyone and everything connected to them.



Silicon Valley venture capitalist Marc Andreessen has said, “software is eating the world,”<sup>[19]</sup> - our new reality is what’s coming out the other end: convenience and connection, and also relentless wars for narrative control, storyweapons of micro-targeted persuasion and behavior modification at scale, and Codespaces of predictive actuation.

Fighting these wars across mental, physical, and Codespace geographies will require new operational models. For example, the ad agency where I work bases organizational structure on slime mold, a networked organism that coalesces from slime into a collective, mobile being, purpose-built to achieve specific goals, which, once achieved, returns to its original state. As the landscape of persuasive communication has evolved, this structure has allowed maximum flexibility and resilience. Another active-defense model is the human immune system, and how it identifies and assesses potential threats, and distinguishes them from healthy tissue.

To “defend the United States against all enemies” means we must effectively counter attacks on our democracy, our institutions, and our people from without or within. We cannot allow the American experiment to “die by suicide” under our watch. General (Ret.) James Mattis noted, “a proper understanding of our national story is absent”<sup>[20]</sup>. In that void we have allowed attack vectors on our societal cohesion to be built around us, enabled by direct access to the minds of American citizens. To counter effectively, our forces must be opportunistic, flexible, and adaptable, able to ‘defend forward’ at home and abroad against enemies domestic and foreign—with a force that is a hybrid of public, private, and military actors, flexible, resilient, and purposeful-built to defend our stories, and to win on the Storyweapon battlefield.

Stories will make or break us. We need storywarriors on the field, fighting for the best version of America. The American story will be pivotal in the decade-to-come as our decisions determine whether Codespace becomes a prison of insular micro-realities, or a launch pad for a greater good. The health and continued viability of the American experiment hinges on the result. We face a nation-wide collapse of journalism (the critical watchdog of a democratic society), accelerating climate disaster, and widening income and opportunity inequality. We will be living with the impact of COVID-19 for years to come, and already, the mis- and disinformation campaigns are ramping up for the 2020 presidential election cycle. Now more than ever, we cannot allow our stories to be written by our adversaries.

This is our chance to take the fight to those who would train Storyweapons on our people—and make others think twice about ever doing it again. We do not always get to choose when we fight, but we do get to choose what we fight for.

*What new stories will we write?* 

## NOTES

1. Sheera Frenkel, Nicole Perlroth, and Kevin Roose, “Tech Giants Prepared for 2016-Style Meddling. But the Threat Has Changed”, *The New York Times*, March 29, 2020, <https://www.nytimes.com/2020/03/29/technology/facebook-google-twitter-november-election.html>.
2. Ciara Curtin, "Fact or Fiction?: NASA Spent Millions to Develop a Pen that Would Write in Space, whereas the Societ Cosmonauts Used a Pencil", *Scientific American*, December, 2006, <https://www.scientificamerican.com/article/fact-or-fiction-nasa-spen/>.
3. Carl von Clausewitz, *On War*, (Penguin Classics,1982), 159.
4. Daniel Kahneman, *Thinking, Fast and Slow*, (FSG Adult; 1st ed., 2013).
5. Matthew Shaer, “What Emotion Goes Viral the Fastest”, *Smithsonian Magazine*, April, 2014, <https://www.smithsonianmag.com/science-nature/what-emotion-goes-viral-fastest-180950182/>.
6. Noah Ganzach and Gloria Mark, “Personality and Internet usage: A large-scale representative study of young adults”, *Computers in Human Behavior*, V.36 2014/07/01, 274–281, [https://www.researchgate.net/publication/262016396\\_Personality\\_and\\_Internet\\_usage\\_A\\_large-scale\\_representative\\_study\\_of\\_young\\_adults](https://www.researchgate.net/publication/262016396_Personality_and_Internet_usage_A_large-scale_representative_study_of_young_adults).
7. Clement Bellet and Paul Frijters, “Chapter 6: Big Data and Well Being”, *World Happiness Report*, (Sustainable Development Solutions Network - March 2019) sec 3.2, “Privacy and Conclusions,” <https://worldhappiness.report/ed/2019/> <https://worldhappiness.report/ed/2019/>.
8. Martin Dodge and Rob Kitchin, *Code/Space: Software and Everyday Life*, (Boston: MIT Press, 2014).
9. Steve Leibson, “IPv6: How Many IP Addresses Can Dance on the Head of a Pin?”, *EDN.com*, March 3, 2008, <https://www.edn.com/ipv6-how-many-ip-addresses-can-dance-on-the-head-of-a-pin/>.
10. “Illusory Superiority” is a cognitive bias referenced in the “Dunning-Kruger effect”, *Wikipedia.org*, [https://en.wikipedia.org/wiki/Dunning%E2%80%93Kruger\\_effect](https://en.wikipedia.org/wiki/Dunning%E2%80%93Kruger_effect).
11. Global figure from “New GSMA Study: 5G to Account for 15% of Global Mobile Industry by 2025 as 5G Network Launches Accelerate”, *GSMA.com*, February 25, 2019, <https://www.gsma.com/newsroom/press-release/new-gsma-study-5g-to-account-for-15-of-global-mobile-industry-by-2025/>; US figure from “Ericsson Mobility Report”, *Ericsson.com*, November 2019, accessed: <https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november-2019.pdf>.
12. George Musser, “Time on the Brain: How You Are Always Living In the Past, and Other Quirks of Perception”, *Scientific American Blog*, September 15, 2011, <https://blogs.scientificamerican.com/observations/time-on-the-brain-how-you-are-always-living-in-the-past-and-other-quirks-of-perception/>.
13. Josh Fruhlinger, “The Mirai Botnet explained: how teen scammers and CCTV cameras almost brought down the internet”, *CSOonline.com*, March 9, 2018, <https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html>.
14. Jon Simpson, “Finding Brand Success in the digital world”, *Forbes.com*, August 25, 2017, <https://www.forbes.com/sites/forbesagencycouncil/2017/08/25/finding-brand-success-in-the-digital-world/#7d22a42e626e>.
15. “Average Time Spent per Day with Total Media (2017-2021)”, *eMarketer*, November 2019.
16. Megan Leonhardt, “The 10 Biggest Hacks data hacks of the decade”, *CNBC.com*, December 27, 2019 - <https://www.cnbc.com/2019/12/23/the-10-biggest-data-hacks-of-the-decade.html>.
17. Scott Brinker, “Marketing Technology Landscape Supergraphic (2019): Martech 5000 (actually 7,040)”, accessed March 15, 2020, <https://chiefmartec.com/2019/04/marketing-technology-landscape-supergraphic-2019/>.
18. Jeff Chester, “Acxiom: "For every consumer we have more than 5,000 attributes of customer data", *Center for Digital Democracy*, January 10, 2014, <https://www.democraticmedia.org/acxiom-every-consumer-we-have-more-5000-attributes-customer-data>.
19. Marc Andreessen, "Why Software Is Eating The World", *The Wall Street Journal*, August 20, 2011, <https://www.wsj.com/articles/SB10001424053111903480904576512250915629460>.
20. James Mattis, “The Enemy Within,” *The Atlantic*, December 2019, 102. 20. James Mattis, “The Enemy Within,” *The Atlantic*, December 2019, 102.





# THE CYBER DEFENSE REVIEW

◆ RESEARCH ARTICLES ◆



# Cyberwar is What States Make of It<sup>[1]</sup>

---

Dr. Martin Libicki

**N**o one there at the time could forget the vicious cyberattack on Venezuela's power systems in March 2019. Four days of chaos ensued. Stores and restaurants closed. Card payments systems were down, with customers asked to pay in dollars. Disrupted public transportation left many unable to get to work. Looting ensued. Seventeen people died in hospitals for lack of electricity.<sup>[2]</sup>

Wait, some of you may be thinking: *what* cyberattack? There is no question that Venezuela's grid had serious problems, but the only evidence that a cyberattack caused these problems was the word of President Maduro. He certainly had political reasons to mobilize his supporters against yet another delivered insult by the US, which has made no secret of its desire to see Maduro go.<sup>[3]</sup> More likely, the power outage reflected the same dysfunctional energy facilities that reduced the average daily oil production rate from nearly 2.5 million barrels in 2015, to a third of that in 2019.

Brazil can tell a similar tale of woe. In 2007, hackers attacked the grid of the state of Rio Grande do Sul, causing severe power outages. The CIA picked up and circulated this story within the intelligence community for two years before it was broadcast by *Sixty Minutes* in 2009.<sup>[4]</sup> Or was it a cyberattack? Once it was reported in the press, Brazil's government denied any such cyberattack, claiming the cause to be sooty insulators, resulting in a fine assessed against the relevant utility.<sup>[5]</sup> So, end of the story? Not necessarily, argue two of the savvier observers on the cyberwar scene (one American and one Israeli); there were known groups that had both an interest in, and a talent for cyberspace mischief, and the government of Brazil would have been embarrassed to admit their success.

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



**Dr. Martin C. Libicki** (Ph.D., U.C. Berkeley 1978) is the MaryEllen and Richard Keyser Chair of Cybersecurity at the U.S. Naval Academy where he teaches cyberwar strategy and cyberspace economics. Prior employment includes having been a senior management scientist at RAND since 1998, focusing on the impacts of information technology on domestic and national security. He wrote three commercially published books: *Cyberspace in Peace and War* (2016, second edition forthcoming), *Conquest in Cyberspace: National Security and Information Warfare* (2007), and *Information Technology Standards* (1994). He is also the author of numerous RAND monographs, notably *Defender's Dilemma*, *Brandishing Cyberattack Capabilities*, *Crisis and Escalation in Cyberspace*, *Global Demographic Change and its Implications for Military Power*, *Cyberdeterrence and Cyberwar*, *How Insurgencies End* (with Ben Connable), and *How Terrorist Groups End* (with Seth Jones). Prior employment includes 12 years at the National Defense University, three years on the Navy Staff as program sponsor for industrial preparedness, and three years for the GAO.

If attacks on the power grid can be faked or hidden, imagine what can be done with other mischief in cyberspace. Cyber-espionage can go undetected for years. Withdrawals from bank accounts can be covered by funds transfers from the embarrassed bank (albeit not legally in many countries). Induced failures in police or intelligence systems may not make the news if such systems are themselves unknown to the public. By contrast, there is no hiding when it is the lights that go out. Nevertheless, the *fact* of a power outage does not prove that a cyberattack caused it—and, while the power company might know, they may not say or be encouraged or even allowed to speak. And, even if a cyberattack is established, attribution can still be an issue.

So far, the only verified cases of electric power loss caused by hacking occurred in Ukraine: two separate incidents in late 2015 and late 2016. But just as the existence of nuclear weapons—even though none have been detonated in war since 1945—has dramatically influenced the security choices of the US, Russia, and China, an imminent threat to knockout electric power could shape future crises. Targeted countries could be coerced or alternatively, they could try to pre-empt attackers by doing likewise. The most frequently discussed way to convert the threat to the electric grid from a notional to a real possibility is to implant malware into the other side's industrial control systems (as distinct from their office and billing systems). Such implants have been likened to Soviet moves to put intermediate-range nuclear-tipped missiles in Cuba, thereby tripling their capacity to strike the US.

So, have countries implanted malware in other countries' electric grids? In 2009, *The Wall Street Journal*, with no evidence beyond "intelligence" sources, reported that Russia and China had done precisely that to the US grid.<sup>[6]</sup>

In late 2014, Admiral Michael Rogers, Commander, U.S. Cyber Command (USCYBERCOM), testified<sup>[7]</sup> that,



“there are nation-states and groups out there that have the capability . . . to shut down, forestall our ability to operate our basic infrastructure, whether it’s generating power across this nation, whether it’s moving water and fuel.” Later that year evidence surfaced that Russian hackers had used tools to penetrate power stations (using Black Energy malware) and corrupted software updates of machinery that sat on electronically isolated (aka “air-gapped”) networks (using Havex malware). In mid-2018, DHS officials reported penetration by Russian hackers of the US electrical system by leveraging the phishing-acquired credentials of suppliers to electrical control systems; “They got to the point where they could have thrown switches” and disrupted power flows.<sup>[8]</sup> Iran has been credited with similar capabilities.<sup>[9]</sup> Some believe that “so many attackers have stowed away in the systems that run the US electric grid that experts say they likely have the capability to strike at will.”<sup>[10]</sup>

It is difficult to know what to make of these claims. The intelligence community keeps secrets for a living. Law enforcement rarely releases sensitive information before trials. Corporations seldom concede that they are victims of hackers, especially of hacks that produced no visible effects. Finding malware is not necessarily an indication of cyberattack, either. The malware could have drifted in from elsewhere. Stuxnet, for instance, appeared in over 100,000 systems outside the Natanz centrifuge plant. A compiler corrupted to produce malware-laden software for a specific supply-chain attack can compromise other software that is unknown to the hackers. While possible, it is quite difficult for hackers who cannot communicate with the malware to time an attack.

At least, claims of extant or impending cyberattacks can be refuted if given time. Anomalous indicators on an employee’s laptop at the Burlington Electric Department . . . were initially mistaken for a deliberate Russian hacking attempt on its electrical power grid.<sup>[11]</sup> That is reassuring to onlookers who remember the accusation, and then the retraction, but what if someone had acted irreversibly on the accusation, before it was retracted?

Matters are foggier if attackers, rather than defenders, claim that implants were installed. In mid-2019, USCYBERCOM gave notice that it was installing implants into the Russian electric grid,<sup>[12]</sup> which the Russians denied,<sup>[13]</sup> claiming that such attacks were thwarted.<sup>[14]</sup> So, is the US capable of taking down the Russian electric grid (e.g., in retaliation for their doing likewise)?

Finally, even if the fact of the disruption and attribution both are indisputable, the message intended by the disruption is subject to multiple interpretations. Consider the hacks of Ukraine's power grid.<sup>[15]</sup> The hack, according to Robert M. Lee and Mike Assante (both teach cybersecurity for SANS) was meant, “to stoke the ire of Ukrainian customers and weaken their trust in the Ukrainian power companies and government.” The article’s author, citing Ukrainian sources, then adds that “[s]peculation has been rampant that the subsequent black-outs in Ukraine were retaliation for the attack on the Crimean substations.” Robert Lee was quoted later in the article considering the possibility that, “the attack on the Ukrainian power

companies was a message to Ukrainian authorities not to pursue privatization," ultimately concluding the message to be: "We want to be seen, and we want to send you a message ... oh, you think you can take away the power [in Crimea]? Well I can take away the power from you." Finally, an attack on the electric grid that caused modest effects could easily be portrayed as one that could have caused major effects but for self-restraint or error: the late 2016 cyber-attack on Ukraine's electric grid opened circuit breakers that were closed an hour later, but analysis of the code suggested that the hackers sought to cause physical damage before power was restored but made several coding errors.<sup>[16]</sup> Oleksii Yasinsky, a Ukrainian cybersecurity researcher, believed the hackers "could have knocked out Ukrenergo's transmission station for longer or caused permanent, physical harm to the grid, he says—a restraint that American analysts like Assante and Lee have also noted."<sup>[17]</sup>

What can we draw from these examples? Based on the Venezuelan incident, one observer concluded, "the inability to definitively discount US or other foreign intervention, whether deliberate or accidental, demonstrates the incredible power of using cyberattacks to target utilities."<sup>[18]</sup> But there is an alternative perspective: it demonstrates the profound impact such cyberattacks have on the public's imagination—which, when coupled with the difficulty of proving who did what and why—illustrates the power that mere *claims* of cyberattack have, either by the attacker or the attacked. There is a reason cyberspace events are mysterious. To paraphrase Ross Anderson<sup>[19]</sup>: airline safety has improved faster than cybersecurity because airplanes crash outside and, by so doing, create facts that cannot be waved away. But computers crash inside, which allows others to understate or overstate what actually took place.

### ***Manipulating Information about Information War Itself is Information Warfare***

The ease with which facts can be manipulated, given the ambiguities and obscurities of cyberspace, means that leaders will be tempted to do just that. Having examined the means of distorting the truth, it is important to understand some of the motives that would prompt such distortions. The degree of manipulation will depend on several variables, including the moral quality of a country's leaders, their ability to maintain a narrative at variance with facts, and the political context within which they operate.

In fairness, the ability to create misperceptions that vary with reality is often unequal. Transparency brings reality and perceptions closer together. So, the leeway of governments to fudge events will vary—directly or via proxies (e.g., power grid operators). Competition among private cybersecurity firms makes it more difficult to advance defensible claims. Conversely, exposure to public opinion creates a gap between perceptions and reality that may be unsupportable. Claims to expert authority are not taken as seriously as (we suppose) before. At least in the West, epistemic closure appears to be growing worse. Despite a clear consensus among the cybersecurity community that imaging servers suffices to understand a network intrusion, for instance, many who take their cues from the leaders they like believe

that shipping servers to a foreign country is a way to hide false flag attacks (e.g., Ukrainians doing what Russians are blamed for).

Adding to the discrepancy has been the tendency of some countries to separate their communications from the rest of the world. North Korea remains isolated. China's Great Firewall is a prime example of selective filtering. Iran is similar in this regard and is contemplating even more isolation.<sup>[20]</sup> Russia recently experimented with closing its Internet off from the rest of the world.<sup>[21]</sup> Early hopes that the Internet would bring the world together and that, in John Gilmore's words, "The Net interprets censorship as damage and routes around it," look nostalgic. As Evgeny Morozov observed in *The Net Delusion: The Dark Side of Internet Freedom*,<sup>[22]</sup> authoritarian governments originally caught flat-footed by the Internet have learned how to control it and turn it to their purposes.

Between the facts that, for laypeople, cyberspace is opaque, and yet, the Internet can actually facilitate misperception over reality, the stage is set for states to make of events in cyberspace as they will.

To simplify the question, consider two players: the target and the attacker. The target has two basic choices: to play up the incident (even, perhaps especially, if no cyberattack were actually involved or no implant dropped), or to downplay it. The attacker has two basic choices as well, but is in a poor position vis-à-vis the target to argue about the effects of the cyberattack. Figuratively and literally, the target is there, and the attacker is not. But the attacker can either dispute or embrace attribution because the requisite evidence is something the attacker will have special knowledge of.<sup>[23]</sup>

The target can play up the cyberattack in many ways. Assuming there is *something* to work with (e.g., a blackout), it can be mischaracterized as an accident, human error, design flaw, as well as a cyberattack. As a variant, an accidental or inadvertent cyberattack can be characterized as deliberate and malicious.<sup>[24]</sup> A cyberattack with a weak effect could be touted as a bullet dodged, either because the hacker erred, or because the hacker was brandishing its capabilities and could have done worse if it wanted to. And, as noted, even if no cyberattack took place, some entity the target wants to malign could be accused of having planted malware "discovered" in the system. Attribution can also be played, largely because some cyberattacks are more embarrassing than others. An inside job can imply that an organization's employees are untrustworthy, or that the organization poorly vetted, and/or that its systems afforded others too many privileges. The victim of a state-backed hacker group can summon the misleading argument that a private company can no more defend its network against an army than it can defend its factory against one; falling to a criminal group is more blameworthy. Finally, if the adverse impact of the cyberattack is insufficient to meet the target's needed political narrative, the cyberattack can be cast as the beginning of a systematic campaign. With a little nerve, it can argue that it was the first shot in a kinetic war, thereby justifying the target's decision to

mobilize its society to fight. While an actual kinetic war may not happen, an action-reaction cycle could actually escalate into war. And if the war does not come, there's always the narrative that war would have come were it not for the target's raising the alarm and mobilizing (e.g., its own forces, the righteous anger of its citizenry, enraged world opinion) accordingly.

This litany of options illustrates why the target may play up a cyberattack. They help unify a country in the face of an adversary while distracting the polity from the government's mistakes. The mobilization of opinion helps governments institute repressive measures or raise taxes. Threats of cyberattacks may persuade the public to allow its government access to personal or organizational systems. Once governments are granted authority to surveil systems for malware or other evidence of intrusion, they can use such access to monitor unwanted activity by citizens. Accusations may create cover for the target's own aggressive acts, forcing concessions from the attacker, even if the incident is phony or exaggerated. It can warn third countries that war may be coming, thereby forcing alliances or other commitments. (Ironically, hyping a cyberattack could lower tensions by substituting conflict in cyberspace, which is unlikely to kill anyone, for more risky posturing in the physical world).

The most innocent explanation is that exaggerating the cyberspace threat will persuade many to take cybersecurity more seriously as they should have from the start (like Senator Arthur Vandenberg, who told President Truman public support for aid to Greece and Turkey against Communists required him to "scare the hell out of the American people"). But this rationale holds some paradox. If the point is to inspire confidence in the integrity of government processes – for instance, that voters can trust election results because they are protected – advertising their vulnerability to hacking may ultimately lead to trustworthy voting systems but, until then, will not produce trusted voting systems.

That logic is one of several reasons' leaders may be reluctant to play up cyberattacks. As a device for mobilizing popular opinion, cyberspace events may be too esoteric, incomprehensible, and removed from daily concerns to allow for galvanizing emotions. Unlike terrorism, cyberattacks more likely will engender anxiety and annoyance, on par with the prospect of a morning traffic jam. But if someone's literal viscera are not threatened, can cyberattacks induce the kind of visceral fear with the requisite political clout?

Reasons to downplay cyberattacks are not hard to find. Falling victim to cyberattacks is, as noted, embarrassing. Such catastrophes can be prevented either by diligent cybersecurity investments or through various forms of self-denial (e.g., closing systems to easy access by others, retaining less information, or prioritizing security over usability and flexibility). Because the point of government is providing security and reliability, admitting that it failed at that can be difficult.

Other reasons for reticence may arise in strategy. Just as playing up cyberattacks may help mobilize citizens for confrontation, playing them down may allow governments to avoid

confrontations they cannot win or at least can win only at great cost. Analogously, many in Europe were eager to accept Putin's assertion that Russia had no forces in Ukraine's east: "[The West] connived in Mr. Putin's pretense that he had not invaded eastern Ukraine—even though in a furtive tricky way he plainly had—because to say otherwise would have required a drastic response."<sup>[25]</sup> Playing down attacks also signals insouciance. Thus, if its purpose is to goad the target into doing something rash (e.g., as the September 11<sup>th</sup> attacks may have been used by al-Qaeda to goad the US into Afghanistan) then downplaying that would translate as an insufficient pain threshold to merit response. Similarly, by refusing to admit to being hurt, a state conveys that it is not coerced and thus will not accede to whatever demands, be they explicit or implicit, are imposed by the attacker, and will itself be undeterred in pursuing its own ends.

Denying attribution also obviates pressures on the target to respond, and also conveys, albeit weakly, that the cyberattack fell below some pain threshold. This allows the target state the option to determine later that they have enough confidence to respond. Conversely, an argument that the pain of cyberattack is limited can be undermined by the discovery of wider and deeper effects and rarely can be assigned by the reverse (much as death tolls can only go up as catastrophes are investigated). The same holds for characterization of near-attacks or failed-attacks. Earlier interpretations that they were not deliberate or carried out by incompetents can be credibly revisited.

A last option is to cast doubt on any early facts, whether helpful or harmful. One reason may be to avoid prejudicing the investigation in the hopes of learning the real lessons for the incident. Another is to prevent the attacker (and would-be copycats) from receiving battle damage assessment so to speak, the better to perfect subsequent attacks.

As to attackers, they, like defenders, can play up or play down the consequences of the attack, its characterization, or its attribution. In practice, however, it is difficult for attackers to more credibly characterize the attack than the target, which has far greater access to information than the attacker. Indeed, the attacker often will have very little if any firsthand information. Reports, for instance, that the US successfully interfered with performance of North Korea's Musudan missile had to be left dangling because of the lack of any sure way to know whether the hack actually worked, or, even if it did work, was a decisive factor in subsequent launch failures.<sup>[26]</sup> The best the attacker can do is to argue that while the target may know better, its leaders often lie about what they know to be otherwise. It took two months after the public learned about Stuxnet for Iran to concede it had been hurt. Yet neither the US nor Israel officially claimed that the attacks succeeded.

In theory, matters are less clear. Attackers usually know better what they tried to do than do defenders; if the damage is subtle or only appears under certain circumstances, the attacker may know to look to telltale signs that its attacks worked, often leaving the defender oblivious to the attack. Subtle attacks also do not make the news, at least not until their impacts become visible.

This leaves attribution as the attacker's primary lever. Countries generally do not acknowledge their cyberspace operations, even when so accused. This stands in contrast to acts of terrorism (at least pre-9/11), which were followed by multiple claimed terrorist *group* perpetrators. Many cyberattacks such as the 2012 attack on Saudi Aramco or the 2014 attack on Sony are claimed by *groups*: The Cutting Sword of Justice and the Guardians of the Peace, respectively. But these groups do not really exist as separate entities. The reasons to deny attribution are straightforward. Most accusations involve cyber espionage whose operators avoid—because the point is to work undetected—revealing their own capabilities and modus operandi.

As for the rarer instances of cyberattack, often the target knows the attacker's identity, while admitting as much opens the attacker to criticism and makes it hard for the attacker to, in turn, criticize incoming cyberattacks. For example, going back at least to the 1973 War, Israel's neighbors believed that Israel had nuclear weapons, thereby giving Israel the benefit of deterrence. Yet Israel strenuously denied having such weapons, to the point of even luring and then jailing Mordechai Vanunu, an Israeli who revealed as much to the British press in the 1980's.<sup>[27]</sup> Israel may well have calculated that open admission would have led third parties to push Israel to de-nuclearize, or to pressure neighboring countries to pursue their own nuclear weapons.


Stuxnet provides an interesting case in contrast. Neither the US nor Israel denied this cyberattack,<sup>[28]</sup> yet neither admitted it officially, at least at first. But at least some in each country wanted to take credit for it. In the US, former Vice Chairman of the JCS, General Cartwright, was accused to have been the source for David Sanger's articles on the hack. And a 2011 YouTube video captured Israel's Chief of Staff at his retirement party counting Stuxnet among his prominent achievements.<sup>[29]</sup> In 2016, an official Israeli document baldly stated, "an example of an offensive cyber operation conducted by Israel is Stuxnet, which was jointly developed with the United States and targeted Iranian nuclear facilities."<sup>[30]</sup> Other governments have tried to have it both ways. Russia denied hacking the DNC in 2016, but its President called the hackers "artists."<sup>[31]</sup> North Korea denied hacking Sony in 2014 but called it a "righteous deed."<sup>[32]</sup>

Generally, hypocrisy—a tribute vice pays to virtue—rules. Given a choice between appearing great and appearing good, countries choose good. That is, they would rather talk up their fealty to international norms than overawe others with their cyberspace prowess. But for how long? As noted, the US did not seem to mind news stories that it had penetrated Russia's grid. In the summer of 2019, the US also indicated it was penetrating systems of those intruding against the US<sup>[33]</sup> (a.k.a. "defending forward," or "persistent engagement"), and had countered Iran's shoot-down of a US drone with a cyberattack.<sup>[34]</sup> Might other countries follow? No country had (publicly, at least) established a cyberspace operations entity until the US formed USCYBERCOM. Many blushed at the thought of militarizing cyberspace until they—first allies, and then adversaries—followed suit. Whether other countries copy the trend

of taking credit not only for successes but also for operations more difficult to assess as successful depends on whether the aforementioned events of 2019 recur. This, in turn, depends on how much they reflected the character of the U.S. Administration at the time. But if such behavior becomes a trend, as opposed to a blip, other countries likely will follow suit in the years to come.

## CONCLUSION

It has been said that the first casualty in war is truth. Today advances in technology and transparency as well as the professionalization of inquiry make it easier to determine the truth sooner rather than later. In this regard, cyberspace lags. Perhaps this should not be so—a fully imaged computer hard drive after a cyberattack leaves nowhere for anything to hide. But, in practice, there is often no third-party confirmation of a successful cyberattack, much less a failed cyberattack, or one partially completed (e.g., an implant). There is no easy equivalent in overhead imagery. And besides, matters once considered settled because of elite scientific consensus are increasingly open to question for a variety of causes (e.g., populism, the Internet's ability to support echo chambers, less influence of traditional media, epistemic closure).

True facts of cyberwar are becoming secondary to misperceptions that governments either shape or influence. Increasingly, cyberwar is becoming what states make of it, and how they package it. That leaves, as open questions, what states *will* make of it. As argued, their options range in efficacy and persistence (in the face of subsequent revelations). The strategies states will employ will, of course, adapt to the circumstances. No hard projections can be made about what the games will look like, but games there will be.<sup>[35]</sup> 

## NOTES

1. Titled in homage to an otherwise unrelated article: Alexander Wendt, "Anarchy is What States Make of It: The Social Construction of Power Politics," *International Organization* 46(02):391-425, March 1992.
2. Description from Tom McKay, "Maduro Says 'Multiple Cyberattacks' Backed by U.S. to Blame for Four Days of Widespread Blackouts," March 10, 2019; <https://gizmodo.com/maduro-says-multiple-cyberattacks-backed-by-u-s-to-b-1833190542>.
3. When China's offer to help bolster the security of Venezuela's grid was rejected, even the Chinese were convinced that no such cyberattack had taken place.
4. This claim (without details) was made by the CIA's Tom Donahue (Thomas Claburn, "CIA Admits Cyberattacks Blacked Out Cities," January 18, 2008; <http://www.informationweek.com/cia-admits-cyberattacks-blacked-out-citi/205901631>) and broadcast (with more details) by the CBS news show, "Sixty Minutes" on June 11, 2009 (<http://www.cbsnews.com/news/cyber-war-sabotaging-the-system-06-11-2009/>).
5. Marcelo Soares, "Brazilian Blackout Traced to Sooty Insulators, Not Hackers" November 9, 2009; [http://www.wired.com/threatlevel/2009/11/brazil\\_blackout/](http://www.wired.com/threatlevel/2009/11/brazil_blackout/).
6. Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, April 8, 2009, 1, <http://www.wsj.com/articles/SB123914805204099085>.
7. Ellen Nakashima, "Foreign powers steal data on critical U.S. infrastructure, NSA chief says," November 20, 2014; [http://www.washingtonpost.com/world/national-security/nsa-chief-foreign-powers-steal-data-on-critical-us-infrast-structure/2014/11/20/ddd4392e-70cb-11e4-893f-86bd390a3340\\_story.html](http://www.washingtonpost.com/world/national-security/nsa-chief-foreign-powers-steal-data-on-critical-us-infrast-structure/2014/11/20/ddd4392e-70cb-11e4-893f-86bd390a3340_story.html).
8. Rebecca Smith, "Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say," July 23, 2018; <https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110> and Colleen Long, "Russian hackers used phishing tools in 2017 attack on grid, July 26, 2018; <https://www.apnews.com/2c17bda4ac704df6be66018197f29912>.
9. Courtney Kube, Carol E. Lee, Dan De Luce and Ken Dilanian, "Iran has laid groundwork for extensive cyberattacks on U.S., say officials," July 20, 2018; <https://www.nbcnews.com/news/us-news/iran-has-laid-groundwork-extensive-cyberattacks-u-s-say-officials-n893081>. See also Andy Greenberg, "The Highly Dangerous 'Triton' Hackers have Probed the US Grid," June 14, 2019; <https://www.wired.com/story/triton-hackers-scan-us-power-grid/>.
10. Garance Burke and Jonathan Fahey, "Iranian hackers breached US power grid to engineer blackouts," December 22, 2015; <https://apnews.com/79f0c976364b4c9dad12c44bba4ccc88>. See also Sue Halpern, "Should the U.S. Expect an Iranian Cyberattack," January 6, 2010; <https://www.newyorker.com/tech/annals-of-technology/should-the-us-expect-an-iranian-cyberattack>.
11. Ellen Nakashima and Juliet Eilperin, "Russian government hackers do not appear to have targeted Vermont utility, say people close to investigation," January 2, 2017; [https://www.washingtonpost.com/world/national-security/russian-government-hackers-do-not-appear-to-have-targeted-vermont-utility-say-people-close-to-investigation/2017/01/02/70c25956-d12c-11e6-945a-76f69a399dd5\\_story.html](https://www.washingtonpost.com/world/national-security/russian-government-hackers-do-not-appear-to-have-targeted-vermont-utility-say-people-close-to-investigation/2017/01/02/70c25956-d12c-11e6-945a-76f69a399dd5_story.html).
12. David Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," June 15, 2019; <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>.
13. Ivan Nechepurenko, "Kremlin Warns of Cyberwar After Report of U.S. Hacking Into Russian Power Grid," June 17, 2019; <https://www.nytimes.com/2019/06/17/world/europe/russia-us-cyberwar-grid.html>.
14. Reuters, "Russia thwarts U.S. cyber attacks on its infrastructure: news agencies," June 17, 2019; <https://www.reuters.com/article/us-usa-russia-cyber-russia/russia-thwarts-u-s-cyber-attacks-on-its-infrastructure-news-agencies-idUSKCNITIU0>.
15. Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," March 3, 2016; <http://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.
16. Joe Slowik, "CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack," August 15, 2019; <https://dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf>.
17. Andy Greenberg, "How an Entire Nation Became Russia's Test Lab for Cyberwar," June 20, 2017; <https://www.wired.com/story/russian-hackers-attack-ukraine/>.
18. From Kalev Leetaru, "Could Venezuela's Power Outage Really Be A Cyber Attack?," March 9, 2019; <https://www.forbes.com/sites/kalevleetaru/2019/03/09/could-venezuelas-power-outage-really-be-a-cyber-attack/#34e80b4e607c>.



## NOTES

19. My interpretation of an argument on the first page of Ross Anderson, "Why Cryptosystems Fail," 1993, <https://www.cl.cam.ac.uk/~rja14/Papers/wcf.pdf>.
20. See, for example, Behrang Tajdin, "Iran letter raises prospect of 'white list' internet clampdown," November 26, 2019; <https://www.bbc.com/news/technology-50563917>.
21. Catalin Cimpanu, "Russia successfully disconnected from the internet," December 23, 2019; <https://www.zdnet.com/article/russia-successfully-disconnected-from-the-internet/>.
22. New York, USA: Public Affairs, 2011.
23. Notionally, if the attacker supports multiple, albeit uncooperative, threat actor groups, or when multiple states attack, the target's knowledge may be incomplete. Practically, this is rare to nonexistent.
24. Some consider this plausible. In 2008, a National Journal story quoted unnamed intelligence sources to argue that a hacker trying to map Florida Power & light, "got carried away and had a 'what happens if I pull on this' moment ... [and]triggered a cascade effect, shutting down large portions of the Florida power grid". The outage was later ascribed to human error. See Shane Harris, "China's Cyber Militia," National Journal Magazine, May 31, 2008, <http://www.nationaljournal.com/magazine/china-s-cyber-militia-20080531>.
25. From *Economist*, "The Siege," July 12, 2014, <http://www.economist.com/news/leaders/21606831-believing-vladimir-putin-has-surrendered-ukraine-would-be-naive-west-must-keep-up>.
26. David Sanger and William Broad, "Trump Inherits a Secret Cyberwar Against North Korean Missiles," March 4, 2017; <https://www.nytimes.com/2017/03/04/world/asia/north-korea-missile-program-sabotage.html>.
27. But see Conrad Duncan, "Netanyahu calls Israel a 'nuclear power' before correcting himself in apparent slip of the tongue," January 6, 2020; <https://www.independent.co.uk/news/world/middle-east/netanyahu-israel-nuclear-pow-er-weapons-iran-crisis-trump-a9272086.html>.
28. See, for instance, Deputy Secretary of Defense Lynn's non-answer in Kim Zetter, "Senior Defense Official Caught Hedging on U.S. Involvement in Stuxnet," *Wired*, May 26, 2011, <http://www.wired.com/threatlevel/2011/05/defense-department-stuxnet/>.
29. Christopher Williams, "Israeli security chief celebrates Stuxnet cyber attack" February 16, 2011; <http://www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyberattack.html> and William Jacobson, "Did Israel Just Admit to Creating Stuxnet?," February 15, 2011; <http://legalinsurrection.com/2011/02/did-israel-just-admit-to-creating-stuxnet/>.
30. "Deterring Terror: English Translation of the Official Strategy of the Israel Defense Forces," Belfer Center Special Report of August 2016; <http://www.belfercenter.org/publication/israeli-defense-forces-defense-doctrine-english-translation>, 48.
31. See Andrew Higgins, "Maybe Private Russian Hackers Meddled in Election, Putin Says," June 1, 2017; <https://www.nytimes.com/2017/06/01/world/europe/vladimir-putin-donald-trump-hacking.html>.
32. Choe Sang-Hun, "North Korea Denies Role in Sony Pictures Hacking," *New York Times*, December 7, 2014, <http://www.nytimes.com/2014/12/08/business/north-korea-denies-hacking-sony-but-calls-attack-a-righteous-deed.html>.
33. Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," February 27, 2019; <https://www.whitehouse.gov/presidential-actions/presidentexecutive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.
34. AFP, "US launched cyber attacks on Iran after drone shootdown: reports," June 22, 2019; <https://news.yahoo.com/us-launched-cyber-attacks-iran-drone-shootdown-reports-232123877.html>.



# Doctrinal Confusion and Cultural Dysfunction in DoD

*Regarding Information  
Operations, Cyber  
Operations, and  
Related Concepts*

---

Dr. Herbert Lin

## ABSTRACT

**T**he doctrinal history of information operations, cyber operations, and psychological operations within DoD is tangled and confused. Moreover, those military specialties rank lower in the DoD pecking order, and those with such specialties are accorded less respect than those specializing in traditional combat arts. These two realities have led to inconsistent usage of these and related terms within DoD and the larger national security community in government as well as in public discourse and, arguably, a misallocation of resources given the importance of the information environment in military operations.

## 1. INTRODUCTION

In a Lawfare posting earlier this year,<sup>[1]</sup> I asked how cyber operations, which are the bread and butter of U.S. Cyber Command's (USCYBERCOM) operational activities, could be regarded as psychological operations. This question was raised by two recent articles on NPR<sup>[2]</sup> and in *The Washington Post*,<sup>[3]</sup> the former discussing past activities of USCYBERCOM and the latter discussing possible future activities. Both articles described these activities as "information warfare," "information operations," "psychological operations," and "influence operations." One obvious question raised by these reports is this: In what sense should these activities USCYBERCOM is contemplating or conducting be considered any of these things?

To the extent these operations seek to influence the behavior of senior Russian or ISIL leadership, they are clearly influence operations. Perhaps the fact that they use information to do so makes them information operations. The influence is psychologically mediated; hence they could be psychological operations. They are enabled by cyber operations



**Herbert Lin** is senior research scholar for cyber policy and security at Stanford University's Center for International Security and Cooperation and the Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution. His research interests relate broadly to policy-related dimensions of cybersecurity and cyberspace, and he is particularly interested in offensive cyber operations and the security dimensions of information warfare and influence operations. Dr. Lin is Chief Scientist, Emeritus for the Computer Science and Telecommunications Board, National Research Council (NRC) of the National Academies, and Adjunct Senior Research Scholar and Senior Fellow in Cybersecurity (not in residence) at the Saltzman Institute for War and Peace Studies at Columbia University. He is a member of the Science and Security Board of the Bulletin of Atomic Scientists, and an elected fellow of the American Association for the Advancement of Science (AAAS). He holds a doctorate in physics from MIT.

that use computer hacking techniques to locate, identify, and possibly manipulate the sensitive personal data of the targeted individuals. Maybe they are information warfare activities, since they seek to respond to an information warfare campaign Russia has waged against the United States and its democratic institutions for a very long time (but first burst into public view during the 2016 Presidential election). On the other hand, *The Washington Post* story was careful to note that the options being considered did not “envision any attempt to influence Russian society at large”—thereby excluding one common understanding of what some of these terms often mean.

These terms sometimes are used interchangeably in public discourse and even within the Department of Defense (DoD) community, but they are not synonymous. These terms also have a confused and tangled history even within the DoD. Some have formal definitions, but in practice and reflecting that tangled history, even those working within DoD do not use them consistently in communicating among themselves or with the public. This inconsistent usage creates confusion within the U.S. Government and within public discourse as well.

## 2. ON DOCTRINE, CONCEPTS, AND TERMINOLOGY

This section reviews in some detail the emergence and evolution of a variety of DoD concepts and terminology relevant to information and information technology systems as reflected in joint doctrine, which is widely regarded as the most authoritative source for the meaning of various terms and how they are used to describe US military thought. “Most authoritative” however, does not always mean entirely coherent or consistent. The complexity of DoD doctrine is such that its various parts evolve at different rates, and hence, over time, doctrine may well suffer from at least a partial lack of synchronization.

## **2.1 The Information Function**

Until 2018, US joint military doctrine recognized six joint functions that were common to operations at all levels of warfare: command and control, intelligence, fires, movement and maneuver, protection, and sustainment. In October 2018, Joint Publication (JP) 3-0 (2017 Incorporating Change 1 from 2018) added the information function.<sup>[4]</sup>

Under JP 3-0 (2017 Incorporating Change 1 from 2018), the information function manages and uses information to change or maintain elements such as perceptions and attitudes to influence desired behaviors and to support human and automated decision-making. Importantly, this publication emphasizes that all military activities produce information, which in turn affects the perceptions and attitudes that drive behavior and decision-making.

The information function includes three sets of activities. The first is understanding information in the operational environment, i.e., the perceptions, attitudes, and decision-making processes of relevant actors informed by an appreciation of their culture, history, and narratives, as well as knowledge of the means, context, and established patterns of their communication.

The second set of activities involves leveraging information to influence the behavior of relevant actors through their perceptions, attitudes, and other drivers; to accurately inform domestic and international audiences to put operations into context and to facilitate informed perceptions about military operations; to counter adversarial misinformation, disinformation, and propaganda; and to attack, exploit, and cast doubt on non-friendly information, information networks, and systems to gain military advantage.

The third set of activities is support of friendly human and automated decision-making, i.e., facilitating shared understanding across the entire force and protecting friendly information, information networks, and systems.

JP 3-0 (2017 Incorporating Change 1 from 2018) notes that information (and C2 and intelligence) apply to all military operations, while the other joint functions may or may not apply depending on the purpose of the operations in question. It calls upon the commander to plan all operations so as to influence relevant actors and to benefit from the inherent informational aspects of physical power, but it takes special note of certain means with which to leverage information: key leader engagement; public affairs; civil-military operations; military deception; military information support operations; operations security; electronic warfare; space operations; special technical operations; and cyberspace operations. As it happens, these means are also key elements of JP 3-13 *Information Operations* (JP 3-13 (2012)) (see Section 2.3 below).

## **2.2 Information Warfare**

Within the DoD, the term “information warfare” was apparently introduced Department-wide in a then-classified DoD Directive dated December 1992 with that term as its subject.<sup>[5]</sup> This directive defined “information warfare” as “[t]he competition of opposing information systems

to include the exploitation, corruption, or destruction of an adversary's information systems through such means as signals intelligence and command and control countermeasures while protecting the integrity of one's own information systems from such attacks."

However, possibly limited by classification, this view of information warfare did not become part of joint doctrine until 1996 with the publication of JP 3-13.1 *Joint Doctrine for Command and Control Warfare*.<sup>[6]</sup> This document defined "information warfare" as "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks."

In 1998, DoD changed the definition of "information warfare" in JP 3-13 *Joint Doctrine for Information Operations* (JP 3-13 (1998))<sup>[7]</sup> to mean "IO [information operations] conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries." This publication also defined "information operations" as "actions taken to affect adversary information and information systems while defending one's own information and information systems." This definition of information warfare is virtually identical in content to what DoD understands today as cyberspace operations, as discussed in Section 2.6. Of particular importance is the fact noted in that section that cyberspace operations (often called cyber operations) are generally understood to involve access to and manipulations of computing or communications technology (both hardware and software).

### **2.3 Information Operations**

The 2006 version of JP 3-13 *Information Operations* (JP 3-13 (2006)) replaced the term "information warfare" with "information operations,"<sup>[8]</sup> which it defined to include electronic warfare, psychological operations, military deception, and operations security in addition to computer network operations.<sup>[9]</sup> The terms added to the definition of information operations were previously part of what DoD had called "command and control warfare" in JP 3-13.1, *Joint Doctrine for Command and Control Warfare*.<sup>[10]</sup> Furthermore, JP 3-13 (2006) expanded information operations to include influencing, disrupting, corrupting, or usurping adversarial human, as well as automated-decision-making while protecting US decision-making.<sup>[11]</sup>

JP 3-13 (2006) also introduced the concept of the information environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information," noting that "the information environment is where humans and automated systems observe, orient, decide, and act upon information, and is therefore the principal environment of decision-making." This information environment includes a physical dimension (i.e., the entities that enable individuals and organizations to create effects), an informational dimension (where and how information is collected, processed, stored, disseminated, and protected), and a cognitive dimension (i.e., the minds of those who transmit, receive, and respond to or act on information). Yet the information environment construct did not play a central role in JP 3-13 (2006).

In 2012, DoD issued JP3-13 *Information Operations* (JP3-13 (2012)),<sup>[12]</sup> which changed the 2006 version in three significant ways. First, it elevated the importance of the information environment since information-related capabilities (IRCs) are defined in terms of their ability to affect the information environment. Second, it changed the focus of information operations from a list of operations to “the integrated employment, during military operations, of IRCs in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.” Third, JP 3-13 (2012) emphasized that information operations are not about ownership of individual capabilities (hence the elimination of the list of activities that constitute information operations) but rather the use of those capabilities to create a desired effect.

More formally, JP 3-13 (2012) defined IRCs as the tools, techniques, or activities that affect the information environment. It also identifies a larger number of capabilities that contribute to information operations: strategic communication, joint interagency coordination group, public affairs, civil-military operations, cyberspace operations, information assurance, space operations, military information support operations (formerly psychological operations, or PSYOP), intelligence, military deception, operations security, special technical operations, joint electromagnetic spectrum operations (colloquially known as electronic warfare), and key leader engagement. Further, within the constructs of JP 3-13 (2012), cyberspace is recognized to be wholly contained within the information environment—the logical implication being that cyberspace operations necessarily affect the information environment and furthermore that cyberspace operations are, in fact, an information-related capability.

In 2014, the DoD issued JP 3-13 (2012 Incorporating Change 1 from 2014).<sup>[13]</sup> Differing from the 2012 version only in its addition of doctrine related to the assessment of information operations, JP 3-13 (2012 Incorporating Change 1 from 2014) predates JP 3-0 (2017 Incorporating Change 1 from 2018) by several years. Thus, it would not be surprising to see the next version of JP3-13 to track the discussion of the information function more closely in JP 3-0.

#### ***2.4 Influence Operations***

The term “influence operations” appears to have no DoD (or U.S. Government) definition. Yet the 2009 RAND study *Foundations of Effective Influence Operations* defines influence operations as the “application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post conflict to foster attitudes, behaviors, or decisions by foreign target audiences that further US interests and objectives.”<sup>[14]</sup> This study also noted specifically that although influence operations usually emphasize communications to affect attitudes and behaviors, they can also use military capabilities, economic development, and other in-real-life capabilities to reinforce these communications. RAND views are not necessarily authoritative, but RAND has been a primary analytical resource for the Department of Defense, though an independent one, for many decades.

## 2.5 Psychological Operations

Psychological operations are a key component of information operations, and the NPR and WP stories both refer to them. JP 3-13.2, *Psychological Operations* (JP 3-13.2 (2010))<sup>[15]</sup> and its follow-on JP 3-13.2 *Military Information Support Operations* (JP 3-13.2 2010 Incorporating Change 1, December 20, 2011)<sup>[16]</sup> define psychological operations (or military information support operations as they are now known in DoD's lexicon) as the conveyance of "selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives." These doctrinal documents also indicate that "it is important not to confuse psychological impact with PSYOP. Actions of the joint force, such as strikes or shows of force have psychological impact but they are not PSYOP unless their primary purpose is to influence the perceptions and subsequent behavior of a TA [target audience]."<sup>[17]</sup> Note also that the definition does not restrict psychological operations to conveying truthful information. For practical or operational reasons (such as the damage to US objectives that might result should lies be discovered), it may be wise to restrict a psychological operation to conveying truthful information, but nothing in the definition requires it.

JP 3-13.2 contains two curious omissions. First, it does not include counterpropaganda activities, which are understood to be activities that identify adversary propaganda (defined as communication designed to influence the opinions, emotions, attitudes, or behavior of any group to benefit the adversary), contribute to situational awareness, and serve to expose adversary attempts to influence friendly populations and military forces. This definition of counterpropaganda was present in JP 3-53, *Doctrine for Joint Psychological Operations* (2003), the predecessor of JP 3-13.2; the term was also eliminated from JP 1-02 DOD Dictionary and Associated Terms in the 2010 version.

Second, the DoD definition of psychological operations in JP 3-13.2 does not explicitly acknowledge the possibility that US audiences (or armed forces) could be the target of adversary psychological operations to influence the emotions, motives, objective reasoning, and ultimately the behavior of US actors—definitions of other DoD operations do incorporate the idea that US forces conduct operations to compromise adversary functions while protecting those same for US forces. It is possible that this omission is directly or indirectly a result of DoD policy: DoD Directive 3600.01 *Information Operations* states explicitly that "DoD IO activities will not be directed at or intended to manipulate audiences, public actions, or opinions in the United States and will be conducted in accordance with all applicable US statutes, codes, and laws,"<sup>[18]</sup> and activities that seek to counter adversary psychological operations could be construed as violating this directive.

## 2.6 Cyberspace Operations

JP 3-12(R) *Cyberspace Operations* was first introduced in 2013,<sup>[19]</sup> and a second revised version published in 2018.<sup>[20]</sup> Both versions define a cyberspace capability as "a device, computer



program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace,” and cyberspace operations as “the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.” Note in particular the technical focus of cyberspace operations.<sup>[21]</sup>

JP 3-12 (2018) states that all cyberspace operations are part of one of three cyberspace missions: DoD Information Network (DODIN) operations, defensive cyberspace operations, or offensive cyberspace operations. DODIN operations secure, configure, operate, extend, maintain, and continuously sustain on an ongoing basis DoD cyberspace, and create and preserve the confidentiality, availability, and integrity of the DODIN. Defensive cyberspace operations defend the DODIN from specific threats that have bypassed, breached, or are threatening to breach DODIN security measures, and defend other cyberspace assets that the DoD has been specifically ordered to defend. Offensive cyberspace operations project power in and through foreign cyberspace. They may exclusively target adversary cyberspace functions, or create first-order effects in cyberspace to initiate carefully controlled cascading effects into the physical domains to affect weapon systems, C2 processes, logistics nodes, high-value targets, and so on.

JP 3-12 (2018) also describes how cyberspace operations contribute to the joint functions of command and control, intelligence, fires, movement and maneuver, protection, sustainment, and, most importantly, information. After repeating the discussion of the information function contained in JP 3-0 (2017 Incorporating Change 1 from 2008), JP 3-12 (2018) describes cyberspace as a medium through which specific information capabilities, such as military information support operations or military deception, may be employed. It notes that while some operations in the information environment may be done using only cyberspace operations, other such operations may not involve them.

### 3. INFORMATION AND CULTURAL DYSFUNCTION IN DOD

It is important to consider the information function itself in relation to the other joint functions. As noted in Section 2.1, JP3-0 (2017 Incorporating Change 1 from 2018) added information as a joint function essential to military operations at all levels of warfare. These other functions are:

- ◆ Command and control, which encompasses the commander’s exercise of authority and direction over assigned and attached forces to accomplish the mission,<sup>[22]</sup>
- ◆ Intelligence, which informs commanders about adversary capabilities, centers of gravity, vulnerabilities, and future courses of actions, and helps commanders and staffs understand and map friendly, neutral, and threat networks,<sup>[23]</sup>
- ◆ Directing fires of available weapons and other systems, which creates a specific effect on target(s), both destructive and non-destructive,<sup>[24]</sup>

- ◆ Movement and maneuver secure positional advantages before or during combat operations,<sup>[25]</sup> and
- ◆ Protection, which helps preserve the fighting potential of the commander's forces.<sup>[26]</sup>
- ◆ Sustainment, which entails logistics and personnel services to maintain operations through mission accomplishment and redeployment of the force.<sup>[27]</sup>

These seven functions are described as essential to all military operations, yet the fact that previous versions of JP 3-0 did not explicitly include information suggests that DoD did not view information to be as important as the others. According to one account provided by a senior military cyber commander,<sup>[28]</sup> the doctrinal authorities recognized that adversaries were accomplishing goals in the operational environment (in which the original six functions resided) solely through activities in the information environment. Adoption of the information function was their way of reconciling the growing importance of information-centric activities with the operational environment and the primacy of the first six functions at the center of previous doctrinal formulations.

As noted in Section 2.1, the description in JP3-0 (2017 Incorporating Change 1 from 2018) of the information function calls for the commander to plan all operations to influence relevant actors and to benefit from the inherent informational aspects of physical power. C2, intelligence, and information are functions that apply to all military operations, but of these three, only information is outwardly relevant—that is, it seeks to influence non-US actors. Furthermore, JP 3-0 (2017 Incorporating Change 1 from 2018) notes that the other joint functions may be necessary only in some other military operations, depending on their scope and goals.

Put differently, information is the only function that is both outwardly as well as inwardly directed and is applicable to all military operations. As the information environment is increasingly overlaid on top of the operational environment, information will be uniquely and increasingly importantly cross-cutting among the joint functions. On the other hand, and despite rhetoric and doctrinal statements to the contrary, US military culture is oriented towards the physical world and the operational environment. It has historically looked to the operational environment as where battles are won, and mass, firepower, and technological overmatch have been regarded as the tools with which to win battles, and physical engagement, courage, and bravery are honored above other personal attributes in soldiers. The patron saint of US military culture writ large is much more Clausewitz, who emphasizes the need to destroy the enemy's means of physical resistance,<sup>[29]</sup> than Sun Tzu, who emphasizes the desirability of winning without fighting.<sup>[30]</sup>

This ethos surfaced conspicuously in February 2013 with the proposed Distinguished Warfare Medal (DWM), introduced by then-Secretary of Defense (SECDEF) Leon Panetta to provide “distinct, department-wide recognition for the extraordinary achievements that directly impact on combat operations, but that do not involve acts of valor or physical risk that combat

entails.”<sup>[31]</sup> By design and intent, this medal was to be awarded not for acts of battlefield valor, but rather, for key contributions to combat operations whether or not within a combat zone. DoD provided two examples of medal worthy acts: a Nevada-based operator of a remotely piloted vehicle flying in Afghanistan, and a Fort Meade-based Soldier who detects and thwarts a cyberattack on a DOD computer system. This medal would have ranked above the Purple Heart and Bronze Star, and below the Distinguished Flying Cross.

Despite DoD’s resolve to avoid having this new medal detract from valor decorations, (e.g., the Medal of Honor, Service Crosses, and Silver Star Medals), serious controversy arose for that very reason. Critics all acknowledged the need to recognize those who contribute significantly to combat operations, but hotly disputed placing the DWM above the Purple Heart and decorations that honor physical bravery. For example, one critic said, “Medals that can only be earned in direct combat must mean more than medals awarded in the rear.”<sup>[32]</sup> Another stated that “to rank what is basically an award for meritorious service higher than any award for heroism is degrading and insulting to every American Combat Soldier, Airman, Sailor or Marine who risks his or her life and endures the daily rigors of combat in a hostile environment.”<sup>[33]</sup> Two months later the DWM was canceled by the incoming SECDEF, Chuck Hagel.

The sentiment underlying such comments is clear—one’s physical bravery is prized over and above the value of one’s contribution to the achievement of US military goals. It is thus not entirely surprising that some do not view soldiers with non-kinetic specialties with the same respect as they do for combat arms troops with specializations in more traditional fields such as infantry, armor, and artillery. Indeed, soldiers specializing in information operations—and especially psychological operations—often report feeling that others regard them with disdain and contempt.

A similar mindset can be found in the debate over physical fitness requirements for cyber soldiers. Several things are unassailable in this debate. First, the ability to “fight” on the cyber battlefield is not highly correlated with one’s physical fitness. Second, the actual conduct of cyber operations can be largely though not exclusively conducted remotely from areas in which physical attributes are again not particularly valuable. Third, higher standards for physical fitness will inevitably result in a smaller pool of those with the skill sets needed for the cyber battlefield. And yet, when the services continue to resist these realities, they degrade their own cyber capabilities—a very clear sign that these capabilities are not as highly valued as other capabilities relevant to military engagement.

Psychological operations have also been singled out for some negative comparisons even among the non-kinetic combat capabilities. In 2011, the term “psychological operations” (PSYOP) was superseded by “military information support operations,” on the directive of then-SECDEF Robert Gates, whose explanation for the name change was that “although psyop activities rely on truthful information, credibly conveyed, the term PSYOP tends to connote propaganda, brainwashing, manipulation, and deceit.”<sup>[34]</sup> Indeed, JP 3-13-2 *Military Information*

*Support Operations*, explains that such operations “create and reinforce actions that are executed to deliberately mislead adversary military decision makers about US military capabilities, intentions, and operations.”

The conduct of psychological operations also tends to require higher authorities than for kinetic operations. For example, during Operation INHERENT RESOLVE, the authority to strike ISIS kinetically required a brigadier general or even below, while an information operation—including a psychological or military information support operation—required the approval of a at least a major general. Indeed, at the start of Operation INHERENT RESOLVE, some such operations required approval at the level of the National Security Council (NSC). Any such operation conducted via the Internet or social media required Pentagon-level approval.<sup>[35]</sup> These constraints have led some to wryly conclude that “it is easier to get permission to kill terrorists than it is to lie to them.”

Organizationally, Army psychological operations personnel constitute most of DoD psychological operations personnel. Most of these Army personnel are under the operational command of the Army Public Affairs and Psychological Operations Command,<sup>[36]</sup> which itself is an Army Reserve command. Only a relatively small fraction of Army psychological operations personnel are active-duty soldiers under the operational command of U.S. Special Operations Command (USSOCOM).

At the level of the U.S. Government, Carnes Lord takes note of American cultural inhibitions with respect to psychological operations,<sup>[37]</sup> pointing to a tendency to “discount the relevance of nonmaterial factors such as history, culture and ideas . . . [and] to assume that concrete interests such as economic well-being, personal freedom, and security of life and limb are the critical determinants of political behavior everywhere, the extreme difficulty of “Americans [in dealing] effectively in international settings where basic American values are under challenge”, a manifest or latent “distaste for any sort of psychological manipulation or deception,” and an idea that psychological operations are “a black art that can be morally justified only under the most extreme circumstances.”

DoD policy also forbids information operations that manipulate audiences, public actions, or opinions in the US. As a result of that policy, DoD cannot directly take actions to mitigate the effects of adversary information-based campaigns against US citizens—it can only act against those responsible for conducting such campaigns, even though as described in Section 2.5 it once had considerable counterpropaganda knowledge and expertise that would be relevant to such a goal.

Tasking DoD to conduct direct defensive operations to protect Americans against foreign influence is beyond the scope of this article, and arguably a bad idea—perhaps even Constitutionally suspect as well. But under existing law,<sup>[38]</sup> DoD can support civilian authorities (e.g., it can help prepare, prevent, protect, respond, and recover from domestic incidents). Thus, DoD cannot act in a counter-propaganda role to protect US citizens from malign foreign influence,

but it can lend expertise and knowledge to civilian authorities, such as the Department of Homeland Security (DHS) or state and local governments, as requested.

#### 4. DISCUSSION

The previous sections highlight some of the ambiguity in public discussions mentioned in Section 1. Cyber operators performing in offensive cyberspace operations are providing fires, yet an offensive cyber operation also can serve to materially impact the decision-making processes of an adversary. When the goal of an offensive cyber operation is to affect adversary decision-making processes, that operation can be regarded as an information operation, specifically a psychological operation.

At the same time, the doctrinal history holds an important lesson for internal DoD discourse about information warfare, information operations, and the like, and communicating with the US public about such topics. Outside the DoD specialist community, the terms “information operations” and “information warfare” have evolved to be more or less synonymous with the deliberate spread of disinformation for adversarial purposes; that is, they are more limited in scope than DoD usage conventions. This is true outside the DoD as well.<sup>[39]</sup> This common understanding of information operations and information warfare is quite similar to DoD’s definition of psychological operations as described in Section 2.5.

Such conflations are not new. In a May 2007 article,<sup>[40]</sup> Curtis Boyd (then assistant chief of staff, G3, at the U.S. Army Civil Affairs and Psychological Operations Command) pointed to the widespread adoption of “information operations” as a euphemism for psychological operations. He observed that “unified combatant command theater security cooperation plans . . . routinely use[d] IO synonymously for PSYOP to describe regional security information programs, activities, and exercises with other nations. . . .” Further he noted several examples of such conflation: a retired major general who wrote that he used IO and PSYOP interchangeably in describing activities in Bosnia; then-SECDEF Donald Rumsfeld describing leaflet drops and Commando Solo broadcasts (typically activities conducted by psychological operations personnel) as IO preparation weapons against Iraq; and the description of a Marine Corps platoon leader of Iraqi troops surrendering as the result of an intense “information operations” campaign that dropped leaflets and broadcasted surrender appeals from loudspeakers.

Although the Boyd article was published in 2007, there is little evidence that such usage has changed in the interim. Indeed, *The Washington Post* article cited above uses the term “information warfare” as being generally synonymous with the activities being conducted, presumably based on interactions with knowledgeable DoD personnel. Apparently, the term “information warfare” is often used to refer to a state-on-state use of cyber-enabled propaganda campaigns aimed at national publics, which is an even more restricted formulation with no obvious analog within the DoD lexicon. It may be true that cyberspace operations as understood within DoD doctrine can be used to deliver psychological effects, but the understanding in common

parlance is that cyberspace operations affect silicon-based machines and psychological operations (as well as information operations, influence operations, and information warfare) that affect human minds.

To sum up, I am suggesting that the history and evolution of doctrinal constructs in these domains have led to a situation in which non-cyber and non-MISO DoD personnel view terms and concepts such as information warfare and information operations more similarly to how these terms are used in societal discourse than to how cyber and MISO specialists understand them.<sup>[41]</sup> Using these same terms differently in different contexts is likely to create conceptual confusion that in turn can also result in misallocation and misalignment of resources and capabilities.

For example, such confusion may make it more difficult to recruit, hire and train the right people due to a lack of understanding about what different missions and skill sets actually entail. If recruiters are unable to clearly articulate what missions entail, they will be unable to hire people whose qualifications are optimized to perform those missions. Similar concerns attach to performance evaluation—without a clear articulation of what effective mission performance means, it is more difficult to differentiate between high and low performers.

Perhaps of greatest significance are the cultural considerations discussed in Section 3 as they potentially affect doctrinal formulations. As that section pointed out, non-kinetic military specializations are not as highly ranked in the DoD cultural hierarchy (aka the pecking order) as kinetic specializations, and it would not be surprising if the lack of respect accorded the former translated into a lack of significant attention to such matters on the part of the latter. Everyone is busy, and for matters deemed of lesser importance, incentives to familiarize oneself with such matters are likely to be scarce.

The comments above reflect a degree of cultural dysfunction within DoD regarding information operations (contrasted with kinetic operations) and more so for psychological operations. Overall, they suggest that the full incorporation of psychological operations into military operations will continue to face an uphill battle within the DoD community.

## 5. CONCLUSION

The *Army Times* reported in late 2019 that U.S. Army Cyber Command (ARCYBER) was proposing to change its name to Army Information Warfare Command,<sup>[42]</sup> quoting Lt. Gen. Stephen Fogarty, Commander, ARCYBER, as saying “Sometimes, the best thing I can do on the cyber side is actually to deliver content, deliver a message. ... Maybe the cyberspace operation I’m going to conduct actually creates some type of [information operation] effect.”

Assuming this is an accurate quote, a careful parsing of words suggests that Lt. Gen. Fogarty’s words are consistent with the comments of Section 4—cyberspace operations are being

used to deliver a psychological effect. These words also coincide with guidance in JP 3-13.2, *Military Information Support Operations*: “Computer network operations [approximately equivalent to today’s cyberspace operations] support MIS [military information support] forces with dissemination assets (including interactive Internet activities) and the capabilities to deny or degrade an adversary’s ability to access, report, process, or disseminate information.”

A name change to Army Information Warfare Command would expand the 1998 definition of information warfare, which Section 2.2 pointed out was essentially synonymous with what are known today as cyberspace operations. Everything that falls within the full scope of the expanded definition of information warfare is unknown (at least to me), but at a minimum, it seems to include psychological operations (or MISO) as well as cyberspace operations.

A similar story appears to be true of the Air Force. The 16<sup>th</sup> Air Force, known as Air Forces Cyber and the Air Force’s Information Warfare Numbered Air Force integrates multisource intelligence, surveillance, and reconnaissance, cyber warfare, electronic warfare, and information operations capabilities across the conflict continuum.<sup>[43]</sup> Prior to its creation in October 2019, one press report quoted a senior Air Force official as saying that “We’ve come to discover cyber is an element of the larger information warfare and [electromagnetic spectrum] fight that we’re in,” and that “to view cyber in its lane and in the functional stovepipe is really an incomplete analysis. We’ve come to discover it’s really information warfare.”<sup>[44]</sup> The same article reported him as saying that the new organization [that is, the organization that would become the 16th Air Force] will focus on “cyber information operations, influence operations, electronic warfare, military deception, military information support operations and psychological operations.”

However, in late February 2020, a search of the 16<sup>th</sup> Air Force web site for “military information support operations” turned up zero references. The word “psychological” yielded one reference—a reference to a component of 16<sup>th</sup> Air Force (the 480<sup>th</sup> ISR Wing) that conducted psychological operations in 1952 and was subsequently deactivated in 1953. The site contains many references to “information operations,” but examination of these references suggests no connection to psychological operations or military information support operations. The site is also replete with references to “cyber,” and the commander of the 16<sup>th</sup> Air Force has a background that is squarely in the cyber domain as the commander of the cyber National Mission Force.

The strongly technical emphasis and history of the DoD cyber warfare community cause me to question whether DoD is well-positioned to embrace and integrate the psychological aspects of information operations.<sup>[45]</sup> Various service cyber commands (including USCYBERCOM) have concentrated on acquiring the technical expertise that cyberspace operations require. This focus has been entirely proper given their missions to date, but the expertise needed to conduct psychological operations goes beyond the skill set of cyber operators. Nor do the various cyber commands appear particularly interested in obtaining such expertise—a keyword search on USAJOBS (conducted in late February 2020) for jobs involving “cyber” and “psychology” or “cyber” and “psychological” turned up nothing, and of 44 jobs listings resulting from a

keyword search on “cyber command,” exactly zero jobs entailed anything remotely connected to psychology.

The DoD needs a standing operational entity that can integrate specialists in psychological operations and in cyber operations as co-equal partners. As my *Lawfare* posting indicated, “bringing to bear the respective expertise of each command [Cyber Command for cyber expertise, Special Operations Command [USSOCOM] for psychological operations] should . . . enhance the synergies possible between cyber-enabled psychological operations and offensive cyber operations, and it would be most desirable if the two commands could partner rather than compete over the cyber-enabled psychological operations mission.”

The “standing” part of this entity (or entities) is essential, as it would recognize the continuing need to conduct such operations against adversaries who believe that open conflict need not have been declared or even started for hostile activity in information space to begin. To cite just one example, former Russian Deputy Chief of the General Staff Lt-Gen Aleksandr Burutin noted in January 2008 that information weapons can be “used in an efficient manner in peacetime as well as during war.”<sup>[46]</sup> Mark Laity, Chief of Strategic Communications, Supreme Headquarters Allied Powers Europe (SHAPE), pointed out that “the Russians use information from a covert stage through six phases of warfare to the re-establishment of victory. Information confrontation is conducted in every phase, including covertly, in peace and in war.”<sup>[47]</sup>

Many military missions today are conducted under the auspices of joint task forces assembled specifically to conduct individual missions. Although these missions generally have well-defined start and end points, there is precedent for standing joint task forces. In particular, a series of joint task forces were established in the late 1990s to deal with the challenges of defending US information assets and projecting power in cyberspace. Joint Task Force-Computer Network Defense (JTF-CND) attained initial operating capability in December 1998 and reported directly to the Secretary of Defense. JTF-CND evolved into Joint Task Force – Computer Network Operations (JTF-CNO) by the end of 1999, and JTF-CNO itself turned into Joint Task Force on Global Network Operations (JTF-GNO) in 2004.<sup>[48]</sup> This history is noteworthy for the similarity of the cyberspace mission set to that of military information support operations—adversaries pose ongoing and continuing challenges both in cyberspace and in human “brain space, and addressing such challenges is a mission that never ends.

A lighter-weight alternative to a standing JTF could call for similarly structured functional components integrated into the geographical commands. As functional components, they would integrate cyber and PSYOP capabilities. As elements of geographical commands, they would be directly responsive to the needs of theater commanders, reducing the likelihood of deconfliction issues arising from the activities of an entity outside the purview of those commanders. The regional expertise needed for effective psychological operations would also



be more readily available with integration into geographical commands. And there is precedent for functional components of combatant commands—in 2005, U.S. Strategic Command (USSTRATCOM) established the Joint Functional Combatant Command for Network Warfare.<sup>[49]</sup>

I am personally agnostic on the specific form of this operational entity, as long as it meets the two requirements of functional integration and permanence. Whether the right construct is a standing Joint Task Force for Cyber-Enabled Military Information Support Operations reporting to the Secretary of Defense, theater-based joint functional combatant commands for cyber-enabled military information support operations, or something else, the DoD needs to move forward organizationally if it is to have any hope of getting ahead of this new form of warfare. ♥

## **ACKNOWLEDGEMENTS**

Pablo Breuer, Edward Cardon, Jessica Dawson, Matt Ellison, Karen Guttieri, Joseph Reeder, Robert Ross, Jennifer Snow, William Spracher, and Michael Warner offered valuable feedback on initial drafts of this paper. I am to blame for any errors in this paper.

**NOTES**

1. Herb Lin, “On the Integration of Psychological Operations with Cyber Operations,” *Lawfare* (blog), January 9, 2020, <https://www.lawfareblog.com/integration-psychological-operations-cyber-operations>.
2. Dina Temple-Raston, “How The U.S. Hacked ISIS,” *NPR.Org*, September 26, 2019, <https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>.
3. Ellen Nakashima, “U.S. Cybercom Contemplates Information Warfare to Counter Russian Interference in 2020 Election,” *Washington Post*, December 25, 2019, [https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9\\_story.html](https://www.washingtonpost.com/national-security/us-cybercom-contemplates-information-warfare-to-counter-russian-interference-in-the-2020-election/2019/12/25/21bb246e-20e8-11ea-bed5-880264cc91a9_story.html).
4. Joint Chiefs of Staff, Joint Publication 3-0 *Joint Operations (2017 Incorporating Change 1 from 2018)*, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_0chl.pdf?ver=2018-11-27-160457-910](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0chl.pdf?ver=2018-11-27-160457-910).
5. Donald J. Atwood, Deputy Secretary of Defense, “Information Warfare,” Department of Defense Directive (DoDD) TS 3600.1), December 21, 1992. A redacted version of this document can be found at [http://www.dod.mil/pubs/foi/ReadingRoom/Other/14-F-0492\\_doc\\_01\\_Directive\\_TS-3600-1.pdf](http://www.dod.mil/pubs/foi/ReadingRoom/Other/14-F-0492_doc_01_Directive_TS-3600-1.pdf). Cited in Michael Warner, “Notes on Military Doctrine for Cyberspace Operations in the United States, 1992-2014,” *Cyber Defense Review* (online version), August 27, 2015, <https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/>.
6. Joint Chiefs of Staff, “Joint Publication 3-13.1: Joint Doctrine for Command and Control Warfare (C2W)” (Washington D.C., February 7, 1996), [http://www.iwar.org.uk/rma/resources/c4i/jp3\\_13\\_1.pdf](http://www.iwar.org.uk/rma/resources/c4i/jp3_13_1.pdf).
7. Joint Chiefs of Staff, “Joint Publication 3-13: Joint Doctrine for Information Operations” (Washington D.C., October 9, 1998), [http://www.c4i.org/jp3\\_13.pdf](http://www.c4i.org/jp3_13.pdf).
8. Joint Chiefs of Staff, “Joint Publication 3-13: Information Operations” (Washington D.C., February 13, 2006), [https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3\\_13\\_2006.pdf](https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf).
9. Michael Warner, US Cyber Command historian, has noted that the phrase “information operations” first replaced the term “information warfare” in the DOD lexicon as the result of then-classified DOD directive (DoDD S-3600.1), even though the actual definition of the term remained the same. See Michael Warner, “Notes on Military Doctrine for Cyberspace Operations in the United States, 1992-2014,” *Cyber Defense Review* (online version), August 27, 2015, <https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136012/notes-on-military-doctrine-for-cyberspace-operations-in-the-united-states-1992/>.
10. Joint Chiefs of Staff, “Joint Publication 3-13.1: Joint Doctrine for Command and Control Warfare (C2W)” (Washington D.C., February 7, 1996), [http://www.iwar.org.uk/rma/resources/c4i/jp3\\_13\\_1.pdf](http://www.iwar.org.uk/rma/resources/c4i/jp3_13_1.pdf).
11. JP3-13, Information Operations, (2006), I-1.
12. Joint Chiefs of Staff, “Joint Publication 3-13: Information Operations” (Washington D.C., November 27, 2012), [https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012\\_iol.pdf](https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_iol.pdf).
13. Joint Chiefs of Staff, “Joint Publication 3-13: Information Operations” (Washington D.C., November 20, 2014), [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_13.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf).
14. Eric V. Larson et al., *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (Santa Monica, CA: RAND Corporation, 2009), [https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND\\_MG654.pdf](https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf).
15. Joint Chiefs of Staff, “Joint Publication 3-13.2: Psychological Operations” (Washington D.C., January 7, 2010), <https://fas.org/irp/doddir/dod/jp3-13-2.pdf>.
16. Joint Chiefs of Staff, “Joint Publication 3-13.2: Military Information Support Operations” (Washington D.C., December 20, 2011), [https://jpsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional\\_Reading/1CI\\_JP\\_3-13-2.pdf](https://jpsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1CI_JP_3-13-2.pdf).
17. JP3-13.2, Psychological Operations, I-1.
18. DOD Directive 3600.01 Information Operations , USD Policy, May 2, 2013 Incorporating Change 1, May 4, 2017 <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/360001p.pdf>
19. Joint Chiefs of Staff, “Joint Publication 3-12 (R): Cyberspace Operations” (Washington D.C., February 5, 2013), [https://fas.org/irp/doddir/dod/jp3\\_12r.pdf](https://fas.org/irp/doddir/dod/jp3_12r.pdf).
20. Joint Chiefs of Staff, “Joint Publication 3-12: Cyberspace Operations” (Washington D.C., June 8, 2018), [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf).

## NOTES

21. Note also that the U.S. government as a whole defines cybersecurity as the “prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.” (See NSPD-54, available at <https://fas.org/irp/offdocs/nspd/nspd-54.pdf>.) Here the technology-centric connotations of the term “cybersecurity” are readily apparent.
22. JP3-0 (2017 Incorporating Change 1 from 2018), III-2.
23. JP3-0 (2017 Incorporating Change 1 from 2018), III-27.
24. JP3-0 (2017 Incorporating Change 1 from 2018), III-30.
25. JP3-0 (2017 Incorporating Change 1 from 2018), III-37.
26. JP3-0 (2017 Incorporating Change 1 from 2018), III-39.
27. JP3-0 (2017 Incorporating Change 1 from 2018), III-47.
28. Lt. Gen. (Ret.) Edward C. Cardon, former Commanding General of U.S. Army Cyber Command (2013-2016), personal communication, February 20, 2020.
29. For example, Clausewitz writes that “Direct annihilation of the enemy's forces must always be the dominant consideration,” (p 228) as “destruction of the enemy’s forces is the overriding principle of war.” (p 258), Carl von Clausewitz, *On War*, edited and translated by Michael Eliot Howard and Peter Paret, Princeton University Press, 1976, <https://press.princeton.edu/books/paperback/9780691018546/on-war>.
30. For example, Sun Tzu writes that “to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.” From Sun Tzu, *The Art of War*, Samuel B. Griffith (tr.), Oxford University Press (1963), 76.
31. Jim Garamone, “Panetta Announces Distinguished Warfare Medal,” *American Forces Press Sources*, February 13, 2018, <https://archive.defense.gov/news/newsarticle.aspx?id=119290>.
32. “VFW Wants New Medal Ranking Lowered,” VFW: Veterans of Foreign Wars, February 14, 2013, <https://www.vfw.org/media-and-events/latest-releases/archives/2013/2/vfw-wants-new-medal-ranking-lowered>.
33. “Military Order of the Purple Heart,” Military Order of the Purple Heart, February 15, 2013, <https://web.archive.org/web/20180621131408/http://www.purpleheart.org:80/News.aspx?Identity=238>.
34. U.S. Marine Corps, “Changing The Term Psychological Operations to Military Information Support Operations” (Washington D.C.: U.S. Marine Corps, December 12, 2011), <https://www.marines.mil/News/Messages/MARADMINS/Article/887791/changing-the-term-psychological-operations-to-military-information-support-oper/>.
35. Cole Livieratos, “Bombs, Not Broadcasts,” *Joint Forces Quarterly*, Number 90, 3rd Quarter 2018, 60-67, <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-90/jfq-90.pdf>.
36. “About Us: U.S. Army Civil Affairs & Psychological Operations Command (Airborne)” (Fort Bragg, NC: U.S. Army Reserve), <https://www.usar.army.mil/Commands/Functional/USACAPOC/About-Us/>.
37. Carnes Lord, “The Psychological Dimension in National Strategy,” in Frank Goldstein and Benjamin Findley (eds.), *Psychological Operations: Principles and Case Studies*, Air University Press, 1996, 73-89, [https://media.defense.gov/2017/Apr/07/2001728209/-1/-1/0/B\\_0018\\_GOLDSTEIN\\_FINDLEY\\_PSYCHOLOGICAL\\_OPERATIONS.PDF](https://media.defense.gov/2017/Apr/07/2001728209/-1/-1/0/B_0018_GOLDSTEIN_FINDLEY_PSYCHOLOGICAL_OPERATIONS.PDF).
38. Joint Chiefs of Staff, “Joint Publication 3-28, *Defense Support to Civilian Authorities*,” Washington D.C., October 29, 2018, [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_28.pdf](https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_28.pdf).
39. For example, Facebook defines information operations as “actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome,” possibly using “a combination of methods, such as false news, disinformation, or networks of fake accounts aimed at manipulating public opinion.” Jen Weedon, William Nuland and Alex Stamos, *Information Operations and Facebook*, Version 1.0, Facebook, April 27, 2017, <https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf>.
40. Curtis Boyd, “Army IO is PSYOP Influencing More with Less,” *Military Review* 87(3): May-June 2007, 67-75, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a575201.pdf>.

## NOTES

41. Christopher Paul reached a similar conclusion in March 2019 on a RAND blog, and one element of his preferred way forward is simply to abandon the term “information operations.” See Christopher Paul, “Is It Time to Abandon the Term Information Operations?,” March 13, 2019, <https://www.rand.org/blog/2019/03/is-it-time-to-abandon-the-term-information-operations.html>.
42. Kyle Rempfer, “Army Cyber Lobbies for Name Change This Year, as Information Warfare Grows in Importance,” *Army Times*, October 16, 2019, <https://www.armytimes.com/news/your-army/2019/10/16/ausa-army-cyber-lobbies-for-name-change-this-year-as-information-warfare-grows-in-importance/>.
43. “Fact Sheet: Sixteenth Air Force (Air Forces Cyber),” October 18, 2019, <https://www.16af.af.mil/About-Us/Fact-Sheets/Display/Article/1957318/sixteenth-air-force-air-forces-cyber/>.
44. Mark Pomerleau, “Air Force Hopes New Organization Can Boost Electronic Warfare,” *C4ISRNET*, April 15, 2019, <https://www.c4isrnet.com/electronic-warfare/2019/04/15/air-force-hopes-new-organization-can-boost-electronic-warfare/>.
45. The discussion here focuses on the psychological aspects. The same may well be true for other facets of information operations.
46. Interfax-AVN news agency, January 31, 2008.
47. “Russia: Implications for UK defence and security,” First Report of Session 2016–17, House of Commons Defence Committee, UK Parliament, July 5, 2016, 17.
48. “Command History,” U.S. Cyber Command, <https://www.cybercom.mil/About/History/>.
49. *op cit*. “Command History,” U.S. Cyber Command.





# Understanding and Pursuing Information Advantage

---

Dr. Christopher Paul

The information environment (IE) and operations in and through the IE are currently a particular point of emphasis within the Department of Defense (DoD). Information is the newest joint function (joining command and control, intelligence, fires, movement and maneuver, protection, and sustainment). The Marine Corps has followed suit and made information a warfighting function, and the Army is considering a similar move. 2016 saw the first DoD *Strategy for Operations in the Information Environment*, and 2017 saw the development of the *Joint Concept for Operating in the Information Environment*, signed and released (and the subject of a capabilities-based assessment) in 2018. Senior leaders across the department have repeatedly expounded on the importance of the IE for military operations and declared it a priority.

Part and parcel of this renaissance surrounding the role of information in military operations are new concepts and terms. One that is prominent in new foundational documents and frequently appears in stakeholder discussions is *information advantage*. This article tries to unpack this concept and explore what it might mean and how it should be thought about by the U.S. Army and the joint force more broadly.

## **“INFORMATION ADVANTAGE” APPEARS FREQUENTLY, BUT IS NOT DEFINED**

The *Strategy for Operations in the Information Environment* makes repeated mention of information advantage, as the purpose of the strategy is to lay out a path for the DoD to “gain advantage in the IE.”<sup>[1]</sup> The strategy includes four lines of effort and a host of other elements that will contribute to creating and sustaining advantage, but spends curiously little attention to what having an advantage in the IE looks like. Similarly, the *Joint Concept for Operating in the Information Environment* is a concept focused on the things required “in order to gain and maintain an information advantage,” but describes only the concepts and capabilities necessary to gain such an advantage, without making clear what the information advantage itself entails.<sup>[2]</sup> The 2018 *National Defense Strategy* mentions information advantage, again without definition or elaboration.<sup>[3]</sup>

© 2020 Dr. Christopher Paul



**Dr. Christopher Paul** is a Senior Social Scientist at the RAND Corporation. Chris received his Ph.D. in sociology from UCLA in 2001; he spent academic year 2001-02 on the UCLA statistics faculty. Chris has developed methodological competencies in comparative historical and case study approaches, quantitative analysis, and evaluation research. His current research focuses primarily on operations in and through the information environment. Recent RAND reports include RR-1166/1-A, *Dominating Duffer's Domain: Lessons for the U.S. Army Information Operations Practitioner*, PE-198, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*, and RR-1925/1-A, *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*. The views and opinions expressed here are his own and do not necessarily reflect the views of the RAND Corporation or its sponsors.

*Information advantage* does not appear anywhere in U.S. Joint doctrine, and so is not defined in the *Department of Defense Dictionary of Military and Associated Terms*. Joint Publication (JP) 3-13, *Information Operations*, comes close, as it defines *information superiority* in a way that includes advantage: "The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."<sup>[4]</sup> *Information advantage* does not appear in current service doctrine, either.

Looking to the doctrinal documents of US allies and partners reveals the term in use elsewhere, and defined there. The United Kingdom Ministry of Defence has a joint concept note with the title *Information Advantage* that also contains a definition: "the credible advantage gained through the continuous, adaptive, decisive and resilient employment of information and information systems."<sup>[5]</sup> This definition is somewhat lacking as far as definitions go, however, as it uses both "information" and "advantage" prominently in the definition, and boils down to defining information advantage as the advantage gained through the employment of information. The Australian Department of Defence includes a definition in its doctrine publication 3.13, *Information Activities*: "An information advantage is a favourable information situation relative to a group, organisation or adversary."<sup>[6]</sup> This is the most robust definition available, but it still begs some elaboration.

Having read these different strategies, concepts, and discussions, I find their overall arguments compelling. I want the joint force to operate more effectively in the IE and to seek and achieve *information advantage*... I'm just not entirely sure what exactly that means.



## INFORMATION ADVANTAGE: I WANT THAT, BUT WHAT IS IT?

Perhaps the term is left un- or under-defined because it is held to be self-evident? *Information environment* is defined, and *information* is broadly understood. *Advantage* is a classic military principle, with Strategist Robert Leonhard reminding us, “The history of human warfare is a saga of continuous attempts to gain the advantage over the foe in battle.”<sup>[7]</sup> The foundation of maneuver warfare is about gaining a position of advantage and seeking to apply strength to weakness to maximize advantage.<sup>[8]</sup> Though classic and foundational, neither “advantage” nor “military advantage” is defined in joint doctrine. “Advantage” repeatedly appears in both *Joint Operations* (JP 3-0) and *Joint Planning* (JP 5-0), but is not defined in either publication. “Position of advantage” also appears in several joint pubs but is not formally defined. In annex A, JP 3-0 notes that the goal of maneuver is “to secure or retain a positional advantage, usually to deliver—or threaten the delivery of—the direct and indirect fires of the maneuvering force.”<sup>[9]</sup>

U.S. Army doctrine makes similarly heavy use of “advantage” without formal definition. The Army Doctrine Publication (ADP) 3-0, *Operations*, comes closest in describing a fairly generic type of advantage, a *position of relative advantage*:<sup>[10]</sup>

4-31. A position of relative advantage is a location or the establishment of a favorable condition within the area of operations that provides the commander with temporary freedom of action to enhance combat power over an enemy or influence the enemy to accept risk and move to a position of disadvantage. Positions of relative advantage may extend across multiple domains to provide opportunities for units to compel, persuade, or deter enemy decisions or actions. Commanders seek and create positions of advantage to exploit through action, and they continually assess friendly and enemy forces in relation to each other for opportunities to exploit. [emphasis in original]

To avoid potential incorrect assumptions about *information advantage* as necessarily a form of positional advantage (since information often lacks a meaningful location or position), I am still left wanting a clear description of advantage or military advantage. Turning to the dictionary reveals the following four definitions for *advantage*:<sup>[11]</sup>

1. any state, circumstance, opportunity, or means especially favorable to success, interest, or any desired end: the advantage of a good education.
2. benefit; gain; profit: It will be to his advantage to learn Chinese before going to China.
3. superiority or ascendancy (often followed by over or of): His height gave him an advantage over his opponent.
4. a position of superiority (often followed by over or of): their advantage in experienced players.

Given the dictionary definitions appear to be quite adequate, the lack of a definition of *advantage* in doctrine and strategic theory may not be an oversight. I am content to allow *advantage* in a military context to be something like “circumstances favorable to success” or “a position

of superiority.” This is consistent with ADP 3-0 on position of relative advantage, which is described as “the establishment of favorable conditions...”<sup>[12]</sup> One thing that is noteworthy about the first dictionary definition is that, under this definition, the advantage is clearly and explicitly a *means*, something that is favorable to prospects of successfully achieving the desired *end*. The “ends, ways, means” construct is quite common in military thinking, and here advantage is circumstances that enable reaching ends, but not an end in itself. This is also consistent with ADP 3-0 and the position of relative advantage, in which such a position “provides” or “enhances” or creates opportunities a commander can “exploit” rather than being something sought for its own benefit.<sup>[13]</sup>

In this, ADP 3-0 is a notable exception, as in many presentations of military theory or discussions of *advantage* (be it *information advantage* or some other form), *advantage* is at least sometimes presented as if it is an end unto itself. Many discussions of maneuver warfare emphasize the gaining of advantage, rather than carrying the logic through and describing the gaining of advantage and then exploiting it to achieve objectives. Similarly, both the *Strategy for Operations in the Information Environment* and the *Joint Concept for Operating in the Information Environment* emphasize gaining an advantage in the IE but stop short of discussing how to use that advantage to accomplish the ends.

Advantage is always good to have, but having the advantage is not the same as accomplishing objectives and achieving desired ends. Is there something else important hiding within the concept of advantage that is not captured by a dictionary or common English-language understanding? Before trying to lash up *information* with *advantage*, I want to unpack “advantage” a little further in the military context.

## ON THE NATURE OF ADVANTAGE

What do we really mean by *advantage*? “Circumstances favorable to success” is fine but is still pretty generic. What kind of circumstances? When a strategy, or a commander, or a soldier seeks an advantage, what is really sought, and how does one go about getting it? By exploring the mechanisms behind traditional and intuitively understood forms of advantage, I hope to provide some levers by which I can pry open a better understanding of *information advantage* later in the article.

Anything that can provide circumstances or conditions favorable to success can be labeled as a form of advantage, and that label is spread quite broadly. In the relevant literature, I have encountered numerous types of labeled advantages, including: numerical advantage; relative advantage; position of advantage; position of relative advantage;<sup>[14]</sup> advantages conferred by geography, or climate, or surprise, or technological advancement;<sup>[5]</sup> temporal advantage; political, economic, or cultural advantage;<sup>[16]</sup> physical, moral, and mental advantage;<sup>[17]</sup> capability advantage, decision-making advantage;<sup>[18]</sup> and, of course, informational or psychological advantage.<sup>[19]</sup> I’m sure there are other forms of advantage, too. In what follows, I unpack, repack,

and discuss some of these and sort them into categories in the hope that some important general characteristics and properties of advantage emerge.

One of the most obvious possible forms of military advantage is a simple numerical advantage. Though history is replete with examples of smaller forces prevailing over larger ones, those smaller forces all had to overcome their opponents' numerical advantage. Quantity has a quality all its own. Numerical advantage belongs to the first category of advantage I have identified, *capacity advantage*. Having more of something than the adversary, or more throughput of something, is a capacity advantage. This can be more troops, more vehicles (either for fighting, or transportation, or both), more ammunition, more logistics capacity, more reserves, or more GDP to contribute to the war effort. Advantages of capacity can contribute to the military principle of mass (be it mass of troops, firepower, effects, etc.),<sup>[20]</sup> and can also be relevant to the law of economy of force.<sup>[21]</sup>

The second category of advantage is *capability advantage*. This category captures the ability to do something the enemy cannot, or at least to do something routinely better than an adversary. Various technological advantages belong in this category, such as having air mobility when the adversary does not or having artillery when the adversary does not. Technological capability advantages need not be absolute to convey advantage: even if both sides have fighter aircraft, the side with *better* fighters has an advantage, as does the side whose rifles have noticeably greater effective range. Capability advantage does not accrue only from better technology, but also from other factors related to capability, such as training, morale, and leadership.

Both *capacity advantage* and *capability advantage* are *persistent advantages*. That is, they stem from some enduring property or characteristic of a force that is unlikely to change dynamically with circumstances. Such advantages are not permanent or wholly unchanging: a capacity advantage like numerical superiority can change if a force is subjected to far higher attrition than its opponent, or if a battle produces an encirclement and mass surrender, or if a commander intentionally divides a force. Similarly, a capability advantage like superior artillery range can fade when competitors develop or procure better guns. Still, these *persistent advantages* can be distinguished from *fleeting advantages*, advantages that are more circumstantial and dynamic.

The category of *fleeting advantage* covers things like positional advantage, temporal advantage, or advantage due to surprise. A position of advantage remains advantageous only until the enemy reorients toward that position or moves away from it. ADP 3-0 explicitly acknowledges that positions of relative advantage are "likely to be temporary."<sup>[22]</sup> Similarly, surprise is often a huge advantage that can beget further advantage through shock and cascading surprise, but eventually, an enemy is no longer surprised. Given time to recover, a surprised foe can restore its equilibrium and deprive its opponent of further advantage due to surprise. The advantage sought in maneuver warfare is most often in the category of *fleeting advantage* (though, of course, the good maneuverist will happily use *persistent advantages* such as superior mobility or dynamic junior leaders to create more *fleeting advantages*).

In addition to being either *persistent* or *fleeting*, advantage can also be *known* or *unknown*. A *known* advantage is one that is understood by or obvious to foes (though the full extent of the advantage may not be known). A numerical advantage is usually known; some positions of advantage, such as forces on higher ground or in a fortified position are also usually typically known unless movement to these positions was concealed. An *unknown* advantage is one that foes or competitors are not aware of, or not sufficiently aware of the details of, to anticipate or respond to the advantage. For example, the existence of a new weapon or vehicle may be known, but the capability advantage it conveys may be unknown. Some positions of advantage rely on being unknown to be effectively exploited: an ambush works because it is unanticipated, and troops in a position where they can surprise, or flank, opposed forces would lose their advantage were their enemies forewarned.

*Known* and *unknown* advantages differ in the mechanisms by which they can be favorable to success. *Unknown* advantages must be exploited to convey any advantage. If a force has no idea their adversary has an advantage, it will remain in ignorance (and unaffected) until something is done with it (like an ambush or highly effective demonstration of new capabilities). *Known* advantages can function through being actively exploited but can also function through *display* or *presentation*. Troops arriving on higher ground will have an advantage in any ensuing combat but may also exert influence on the battlefield strictly by their observed presence, as the opposed commander may choose to withdraw forces from the vicinity of the hill. *Known* advantages can contribute to shaping or deterrence even if they are not explicitly exploited.

In addition to these categories (capacity and capability, persistent vs. fleeting, known vs. unknown), advantage appears to have several properties. First, *advantage is always relative*. If “circumstances favorable to success” was a good start on a definition of advantage, a more comprehensive definition needs to include an opponent or other opposition, someone who will resist the accomplishment of the end or objective. The extent to which capacity or capability conveys an advantage is dependent on the relative capacity and capability of the adversary, as is the duration of one’s advantage.

Second, *advantage is always conditional*. Just because one has a certain general advantage does not necessarily mean it is going to give any benefit (that is, be favorable to success) in every situation. Being able to increase prospects for success based on superior capacity or capability, or based on position, depends on the end being sought and on other conditions. For example, night vision equipment only conveys advantage in the dark, and an advantage in weapon range is not an advantage when engagement range is inside both sides’ weapons’ maximum range, such as in jungle or other dense terrains. Similarly, a host of advantages in sea power (numerical, technological) is not advantageous for land operations far from the coast. Often, advantage is conditioned on time (the main distinction between *persistent* and *fleeting* advantage, and what can determine just how fleeting a fleeting advantage is). Left enough time to react, an enemy will try to deprive adversaries of advantages—either the

years it takes to develop a counter-technology or the much shorter amount of time it takes a formation to reorient to a foe on its flank or to move away from a position of enfilade or other positional disadvantage.

The third property of advantage is that *benefit from advantage comes from exploiting it*. Consider the language of advantage: one *takes* advantage, or one presses one's advantage. The benefit from advantage comes from the verb action associated with it. Advantage may be circumstances favorable to success, but if one does not seize on that advantage and exploit it to progress actively toward objectives, one has failed to take advantage. Similarly, forces placed in a position of advantage that fail to act on or exploit that advantage, lose the advantage. *Having* an advantage is nice, but *taking* advantage gets you something. Of course, sometimes, you can capitalize on an advantage simply by *displaying* it. The defensive advantage of a fortified position presents an adversary with a dilemma: either attack the strong point at great cost or decline to pay that cost and leave the defense intact. Either outcome is favorable to the defender.<sup>[23]</sup> Displaying an advantage (that is, allowing it to become a *known* advantage, or presenting the capability related to a known advantage) can shape or deter an adversary's behavior. Moreover, the type or quality of advantage gained may depend on whether it is an advantage *pressed* or an advantage *displayed*, or it may depend on the adversary's choice. When presented with a dilemma, an adversary will choose an available course of action, but may not choose the one most preferred by the force holding an advantage. Still, the nature of a dilemma is such that the advantaged force should stand to gain in some way regardless.

A fourth property of advantage is that *the best advantages match strength against weakness, rather than just overmatching strength against strength*. The best technological advantages do not just let one do something the adversary can do, but better; the best technological advantage lets one do something the enemy cannot do *at all*. Similarly, having a local firepower advantage is a good thing, but being able to direct firepower into an unprepared and undefended enemy is even better. Therefore, advantage is foundational in maneuver warfare, as maneuver always seeks to pit strength against weakness, to dislocate enemy strength and to put often otherwise relatively evenly matched forces in a position of advantage relative to foes.

The fifth and final property is that *advantage is a means, not an end*. Although this was mentioned earlier, it merits repeating as a property. Not only is advantage a means and not an end, but it is also conditional on the nature of the end. For example, if the tactical objective is clandestine monitoring of a route, a numerical advantage is no advantage at all, as it is much harder to hide a large force than a small one. Similarly, a firepower advantage is not much of an advantage when conducting a humanitarian assistance mission. What constitutes advantage at the tactical, operational, and strategic levels will vary in part because the nature of objectives at the tactical, operational, and strategic levels vary, and so too will the kinds of things that are favorable to success in those different levels of objectives.

## WHAT DO WE MEAN BY “INFORMATION”?

Having described some categories of advantage and having offered some properties of advantage, I now turn to *information*. *Information* is used even more frequently in doctrine than *advantage* and is discussed and defined therein. In fact, JP 1-02 includes fully ten separate terms that begin with the word “information” and even more that include it as a second or subsequent term, and even more still that include “information” in their definitions. The information environment is “the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.”<sup>[24]</sup> Though defined, *information* is an incredibly broad term. Taking a term as broad as *advantage* and putting it next to a term as broad as *information*, it is no wonder that *information advantage* threatens some ambiguity.

Information in warfare and other military operations covers a very broad space. To make some sense of what is meant by *information advantage*, we need to parse some of the disparate things that gather under the broad tent of “information.” I have identified at least six different ways in which “information” is described as relevant in warfare or other military operations: (1) situational awareness and situational understanding; (2) command and control, including communications and knowledge management; (3) command and control warfare (C2W) and other factors that degrade situational awareness or C2; (4) information or aspects of the IE that can cause subordinates to behave in ways contrary to the commander’s orders or preferences; (5) efforts to protect against the factors of (4) or inflict them on adversaries; and (6) factors in and through the IE that affect the perceptions or behaviors of relevant actors other than adversaries.<sup>[25]</sup> Each is described in greater detail below.

The first category of information in warfare is information about the operating environment or battlespace, where one’s forces are, where enemy forces are, where other relevant actors are, the state of those actors or forces, and what features of the environment might affect operations. This is commonly described as situational awareness or situational understanding, and during actual operations is opposed by the natural forces of uncertainty collectively called “the fog of war.” The fog of war is fought through sensors and intelligence, surveillance, and reconnaissance (ISR). Opposition from opponents is separated as a distinct category (category 3).

The second category of information concerns command and control, especially the ability to communicate and transfer changes in understanding and instructions. This category recognizes the truth that the commander in the headquarters does not know about contact with an enemy formation the exact moment the first scout in the field spots the first sign of movement, but that there are delays inherent in the system as new ISR is received, digested, and disseminated, and similar delays as orders are developed and communicated to subordinates. This category of information depends on networks and nodes, communication radii, chains of command, numbers of echelons, etc. This category also includes knowledge management, the integration of both new information and old information into meaningful information, and then making that available to those who need it to support their decision-making.

The second category of information concerns command and control, especially the ability to communicate and transfer changes in understanding and instructions. This category is about the sharing of information (specifically ISR and orders) between commanders and subordinates and delays and impediments to that sharing. Because information takes time to pass between echelons, a commander in a higher headquarters will not know about contact with an enemy formation the exact moment the first scout in the field spots the first sign of movement. Similarly, once headquarters becomes aware of a change in the situation, it will take time for new orders and instructions to reach the tactical edge. This category of information depends on networks and nodes, communication radii, chains of command, numbers of echelons, etc. This category also includes knowledge management, the integration of both new information and old information into meaningful information, and then making that available to those who need it to support their decision-making.

The third category is a subset of what is often called *information warfare*. It is an important transition in these categories of information from describing things forces need to at least some extent to operate (the first two categories) to describing an optional activity: fighting with, or against, information. This category is about attacking the functioning of categories (1) and (2). This category includes what has historically been called *command and control warfare* (C2W) and includes other attacks on situational awareness/situational understanding or the systems that convey that knowledge.<sup>[26]</sup> Thought about differently, this is about using information capabilities to amplify the fog of war either to promote general uncertainty or to lead enemies to specific incorrect conclusions about some aspect of the location, disposition, and possible courses of action of friendly forces.

The fourth category is about information or aspects of the IE or operating environment that can cause subordinates to behave in ways contrary to a commander's preferences. This exposes another important relationship with information: namely, how information affects behavior. Why might subordinates not do what a commander wants? There are numerous possible reasons. Subordinates might not know what a commander wants because of failures in C2 (category 2), or because of inflicted failures in C2 (category 3). Subordinates might be incapable of following a commander's orders (if they lack sufficient fuel or ammunition or have sustained so much damage that they are physically disrupted), but the commander may not know that because of failures in situational awareness. Subordinates might perceive the situation differently than the commander (either correctly or incorrectly, but differently) and thus act following the principles of mission command and in a way that is consistent with the overall commander's intent and that subordinate's perception of the situation. Subordinates might also act in contravention of the commander's wishes due to factors that are not strictly rational and are governed by psychology or emotion. This could be the baseline personality and proclivities of a subordinate (bold, or timid, or reckless), or due to effects wrought by battlefield circumstances such as distraction, suppression, panic, fear, shock, surprise, or rage.

The fifth category of information concerns things done in or through the information environment to mitigate or counter the effects of (4) on one's own forces, or to inflict such effects on adversary forces. One might call this "information for effect." This encompasses more of the range of possible operations in the IE and includes efforts to harness the inherent informational aspects of military operations, as well as the employment of various information-related capabilities to affect and influence enemies.

The sixth and final category is factors in and through the IE that affect the perceptions or behaviors of relevant actors other than adversaries, basically category (5) against targets other than enemy troops. This could include other actors in the immediate operating environment (such as non-state actors, or relevant civilian populations, or partner-nation forces) or relevant actors outside the area of physical operations (such as the domestic constituencies that support the adversary, or one's own domestic constituents, or senior leadership/national command authority on either side, or citizens and leaders in nations not a party to the conflict that contribute to the overall accord of international legitimacy). This category is fairly like (5) but includes a broader scope, not only geographic scope but types of relevant actors and timescale as well. While (5) is more focused on things that affect action and behavior in combat, this category includes things that affect perceptions and behavior more broadly and over time. Thus, this category requires tracking and understanding things like narratives, baseline attitudes, and legitimizing processes. Of course, narratives and other longer-term processes can also contribute to shaping baseline proclivities or vulnerability to other effects; thus, they might blur into other categories as a minor influence.

These six categories are distinct but also contain other divisions. Notably a division between rational processing of information and decision-making under various human conditions, such as culture, personality, individuality, psychology, emotion, stress, etc. Categories (1), (2), and (3) all focus on rational processes, and assume that units and subordinates will do what they "should" based on their situational awareness and their orders. Category (4) crosses the boundary and allows that various units and subordinates might have different rationales in their rationality, or might do things based on psychology, personality, or circumstances. Categories (5) and (6) are also on the human conditions side of this division.

Each of these different kinds of information can support different kinds of advantages. By reviewing each of these categories of information in light of what we have already discovered about advantage, we can put some further bounds on *information advantage*.

## **PUTTING IT ALL TOGETHER: INFORMATION ADVANTAGE**

To review: I have offered six categories of advantage (capacity and capability advantage, persistent vs. fleeting advantage, known vs. unknown advantage), five properties of advantage (relative, conditional, active/displayed, best when asymmetrical, and a means not an end), and six categories of information (1 - situational awareness, 2 - command and control, 3 - factors that degrade C2 and SA, 4 - factors that cause subordinates to behave contrary to orders, 5



– efforts to prevent or impose that, and 6 – efforts to affect perceptions and behaviors more broadly). The Table summarizes the *information advantage*.

Table 1: Categories and Properties of Advantage, Categories of Information

Properties of Advantage	Categories of Advantage	Categories of Information
Relative	Capacity	(1) Situational awareness
Conditional	Capability	(2) Command and control
Must be exploited	Persistent	(3) Factors that degrade C2 and SA
Best when asymmetrical	Fleeting	(4) Factors leading to contrary behavior
A means not an end	Unknown	(5) Efforts to affect behavior
	Known	(6) Efforts to affect behavior more broadly

In this section, I review each of the six categories of information looking to provide some specificity or categories of things that might constitute *information advantage*.

Beginning, then, with situational awareness. One can have *persistent advantage* in both *capability* and *capacity* regarding situational awareness, having more sensors, better analytic capability, systems that update more rapidly, etc. Advantage relative to a competitor might come from extending awareness over a greater area, or with greater fidelity, or with greater tempo (either refreshing more frequently, or with fewer delays between sensing and updates to the common operating picture), or through better interpretation or understanding of what is sensed. Likely related to better general capability and capacity (but not necessarily), one might also have a *fleeting* advantage in situational awareness, successfully finding and fixing an elusive, high-value individual, or gaining indications and warnings of a planned enemy movement or aggressive action. The side with the general advantage in situational awareness will not always have the advantage regarding the discovery of every position and movement by the other side, as fewer, less capable systems can still be in the right place at the right time. Advantage in situational awareness can be both *known* and *unknown*, or even a mix of the two. A commander might know an opponent has generally better ISR, but not know if it has detected his/her flanking force; this knowledge of the opponent’s superior ISR might prevent him/her from attempting to send a flanking force in the first place, expecting that his/her forces will be detected and countered. Advantage in this category comes from more and better ISR, perhaps combined with good fortune or other favorable circumstances.

Command and control advantages generally stem from relative reach and speed of decisions, and the communication of them. Commanders who can more rapidly formulate and convey orders to subordinate echelons than their enemies gain the advantage, and commanders who are in communication with more of their more distant subordinate forces than their enemy similarly gain an advantage. Command and control advantage is central in Colonel John Boyd’s thinking about warfare as embodied in the OODA loop (observe–orient–decide–act).<sup>[27]</sup> Advantages in the

tempo of situational awareness and command and control (cycling OODA faster than the opponent) will eventually cause an adversary to fall behind and thus surrender other advantages.

C2 advantage can be both *persistent* and *fleeting*, and sometimes both. A persistent capability advantage in C2 leads to generally faster and more efficient decisions and communications but can also produce a fleeting advantage in which the commander of the force with advantage can perceive and react to changing circumstances before its opponent can. Many forms of C2 advantage involve tempo, either the actual tempo of decision-making or the potential tempo supported by the information, networks, and systems. Note that just because one *can* OODA faster than the opponent does not necessarily mean that you are doing so at any given moment: an indecisive commander within a superior situational awareness and command and control system can still cede the initiative (and thus the advantage).

The use of a C2 system that involves mission tactics, mission command, or mission-type orders can provide an advantage over those which do not. Under mission command, even when out of communication and unable to receive orders from higher echelons, subordinate leaders continue to act based on their understanding of the situation and the commander's intent.<sup>[28]</sup>

Forces that do both category 1 (SA) and category 2 (C2) better than their foes will have a consistent and persistent advantage: decision advantage. The force with better SA and C2 will usually make decisions faster (due to an advantage in decision speed) and better (due to an advantage in decision quality). Not every decision will be optimal or without delay but, on average the side with decision advantage will make better, faster decisions.

Information categories 1 and 2 focus on doing things (SA and C2) better than an opponent. Information category 3 makes this a contested competition, including activities that degrade others' SA and C2 (or protect one's own C2 and SA from such efforts). This includes efforts to deceive sensors (such as camouflage or decoys), efforts to prevent sensors from reporting (such as the destruction, jamming, or hacking of reporting networks), and efforts to promote mistaken conclusions about what is observed. This also includes efforts to avoid exposing plans and actions, such as counterintelligence, operations security, and signature management. This includes any effort to corrupt or slow enemy OODA, including efforts to jam or interrupt conveyance of orders (the seam between deciding and acting, where the decision must be conveyed to those who should act). Further, anything that can threaten the confidentiality, availability, or integrity of information or information systems could contribute to this category.

Advantage in the third category comes from persistently better capability (either ISR capable of piercing enemy deceptions, or sophisticated equipment routinely able to avoid detection or otherwise affect adversary systems), or as fleeting advantages through clever combinations of stratagem, ruse, and thoughtful application of capability. Known and unknown advantages can be particularly powerful here. If one side has a known advantage in stealth or camouflage, the other side may not fully trust its own situational awareness and thus cede further advantage to the advantaged force. An unknown and undetected advantage could

allow a force to affect enemy SA or C2 without their knowledge, enabling extensive further advantage through the manipulation of enemy perceptions and actions. When seeking to deny an opponent of decision advantage, anything that threatens either decision speed or decision quality can be effective.

The fourth category of information encompasses factors that might make a subordinate act in a way that is inconsistent with the preferences of superiors. Advantages in this category stem from aspects of context and from persistent qualities of forces. Better leadership, better morale, better training, and combat experience could convey advantage in this area. Other effects of operations, such as reduced communications availability, casualties, shock, surprise, and suppression, can also convey a fleeting advantage to the side suffering less from these effects. To unpack sources of advantage related to category 4 requires the inclusion of category 5, efforts to intentionally promote contrary behavior. In this related category, advantage could come from the intentional use of shock or surprise to promote a rout, or the combination of various physical and informational capabilities to increase the likelihood of desired battlefield behaviors. Advantage in this category falls to the side that better understands the human, cultural, and other dynamics that drive battlefield behavior and best exploits them. A persistent capability advantage in understanding human dynamics may lead to repeated fleeting advantages as windows of opportunity to leverage that understanding through the application of other capabilities. Further advantage might accrue to the side which seeks to scrutinize and better understand the individual enemy subordinate leaders whose preferences and proclivities might be leveraged. Advantage in this category also falls to the side that emphasizes moral and mental effects from combat and other operations, and specifies objectives in terms of actions desired from enemy forces; over a side that employs attritionist thinking and focuses only on the physical effects of combat.

The sixth and final category of information includes factors and efforts that influence a broader range of relevant actors, including government authorities, civilian constituencies, and non-combatants in an area of operations. While these sorts of groups and individuals are certainly affected by the presence and action of military forces, advantage in this category likely accrues on the side that has better messaging and engagement (whether by the military, across other parts of government, or leveraged in partnership with civil society). Further advantage likely accrues to the side whose relevant actors and supporters are most resilient to influence and manipulation. Similarly, the side whose objectives require only modest influence to achieve, or whose objectives can be met through the influence of groups predisposed toward the desired behaviors, are also advantaged. This is an area in which both capability and capacity advantage are relevant, as a small number of excellent influencers will likely not be advantaged against a much larger number of only adequate influencers. In this category, quantity clearly has a quality all its own.<sup>[29]</sup>

As is the case in other information categories, persistent capability or capacity advantage does not ensure advantage in all instances across this category. Some efforts from the side with lower capability and capacity will still lead to advantageous results, especially with some groups and populations. Further, the uncertainty associated with human dynamics and influence will sometimes cause success to follow the side with a less apparent relative advantage in this category.

### **CONCLUSION: SPECIFY THE INFORMATION ADVANTAGE SOUGHT**

On further reflection, I am now wholly convinced that the joint force should seek to establish and maintain information advantages, but that greater specificity is required in that pursuit. Advantage is a means to an end; it needs to pertain to specific objectives relative to (or over) specific adversaries and competitors. I have identified six categories of advantage and six categories of information. Future discussions of “information advantage” would do well to specify what kind of advantage is desired in which category of information, and relative to whom. Here are some examples of specific forms and objects of information advantage:

- ◆ The US tradition of mission command gives US forces a persistent command and control advantage over Russian forces trained on Soviet models when communication networks are degraded; the joint force should seek to sustain the factors that contribute to that advantage.
- ◆ Russia’s propaganda apparatus demonstrates a persistent capacity and capability advantage over the United States and NATO allies in the area of influencing perceptions and behaviors of various civilian groups by virtue of the large number of distribution sources and modes they employ, their willingness to employ them, and their understanding of human dynamics and societal vulnerabilities; the United States should seek ways to reduce this advantage.
- ◆ US cyber capabilities might provide a capability advantage in the area of affecting an adversary’s command and control and situation awareness during major combat operations that is presently unknown to near-peer competitors; the US should seek to grow this potential advantage and sustain its status as an unknown advantage.

These are just examples. They are not meant to suggest priorities or specific ways the US should seek information advantage, but only to demonstrate the shape of expressions of information advantage that specify the type of advantage, the type of information, and over whom advantage is sought. I encourage stakeholders across the joint force to be similarly specific when thinking, speaking, and writing about information advantage. I am sure there are additional relevant categories of advantage, and possibly additional relevant categories of information, than the ones I have identified here. I would be very pleased to see the lists expanded through use.

## NOTES

1. U.S. Department of Defense, *Strategy for Operations in the Information Environment*, Washington, D.C., June 2016, 4.
2. *Joint Concept for Operating in the Information Environment*, Washington, D.C.: U.S. Joint Chiefs of Staff, July 2018, preface.
3. *Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge*, 6 & 8.
4. Joint Publication 3-13, *Information Operations*, Washington, D.C.: U.S. Joint Chiefs of Staff, incorporating change 1, November 20, 2014, GL-3.
5. Ministry of Defence, *Information Advantage*, Joint Concept Note 2/18, November 2018, 7.
6. Australian Department of Defence, *Operation Series: Information Activities*, Australian Defence Doctrine Publication 3.13, third edition, 2013, 1-3.
7. Robert R. Leonhard, *The Principles of War for the Information Age*, New York: Ballentine Books, 1998, 54.
8. See the discussion of Maneuver Warfare in Marine Corps Doctrinal Publication 1, *Warfighting*, Washington, D.C., June 20, 1997.
9. Joint Publication 3-0, *Joint Operations*, Washington, D.C.: U.S. Joint Chiefs of staff, incorporating change 1, October 22, 2018, A-2.
10. Headquarters, U.S. Department of the Army, *Operations*, Army Doctrine Publication 3-0, Washington, D.C., July 2019, 4-5.
11. Four definitions for advantage, dictionary.com.
12. Headquarters, U.S. Department of the Army, *Operations*, Army Doctrine Publication 3-0.
13. Ibid.
14. Ibid.
15. From Marine Corps Doctrinal Publication 1, *Warfighting*, Washington, D.C., June 20, 1997.
16. Leonhard, 58.
17. Jim Storr, *The Human Face of War*, United Kingdom: Continuum, 2009, 94.
18. UK JDN 2/18, *Information Advantage*.
19. Mentioned in the 2018 NSS, as well as other places.
20. Antulio J. Echevarria II, *Military Strategy: A Very Short Introduction*, Oxford University Press, 2017.
21. See John Frederick Charles Fuller, *The Foundations of the Science of War*, London, Hutchinson, 1926; reprinted by Forgotten Books, 2018, and Robert R. Leonhard, *The Principles of War for the Information Age*, New York: Ballentine Books, 1998.
22. Headquarters, U.S. Department of the Army, *Operations*, Army Doctrine Publication 3-0, Washington, D.C., July 2019, 4-5.
23. If one of the outcomes is *not* favorable to your success, then your enemy can easily thwart your advantage. Consider, for example, the World War II-era German offensive through the Ardennes to avoid the Maginot Line.
24. JP 3-13, ix.
25. These six categories and their description are drawn from Christopher Paul, Yuna Huh Wong, and Elizabeth M. Bartels, *Opportunities for Including the Information Environment in U.S. Marine Corps Wargames*, RAND Corporation: Forthcoming.
26. Consider some of the examples provided in Patricia Frost, Clifton McClung, and Christopher Walls, "Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum," *The Cyber Defense Review*, Spring 2018, 15-26.
27. See, for example, John R. Boyd, "The Essence of Winning and Losing," unpublished briefing, June 28, 1995.
28. Headquarters, U.S. Department of the Army, *Mission Command*, Army Doctrine Publication 6-0, Washington, D.C., May 2012.



# Information Weapons: Russia's Nonnuclear Strategic Weapons of Choice

---

Timothy L. Thomas

## INTRODUCTION

For many years now, Russia has defined and even expanded its concept of “information weapons (IWes).”<sup>[1]</sup> At one point, Russia attempted to get the concept introduced into United Nations resolutions, which at the time helped to guarantee Russian information and national security. This occurred in the 1990s when Russia was at its weakest and unable to compete with other nations in information warfare capabilities. At this time, Russia’s information warfare weakness was so pronounced that a prominent Russian scientist stated the following at an international conference in Moscow in 1995:

In studying the potentially catastrophic consequences from an enemy’s use of strategic information warfare systems on, for example, the economy or government control...we must unequivocally declare that in the case of their use against Russia, we reserve the right to conduct a first strike (nuclear) against the information warfare system and forces which are directing that weapon, and then also against the aggressor-government.<sup>[2]</sup>

This stark warning was intended to send a message to other nations, and it served its purpose well. “Don’t mess with Russia” if you want to keep Russia from messing with you.

Since the revival of Russia’s military prowess, a variety of its authors have continued to focus on information-related topics, to include the following: information warfare, information struggle, information resources, information confrontation, information sphere, information field, information effects, information superiority, information security, and, in line with the focus of this article, IWes. At times, IWes address the information-related technologies used in precision-guided and reconnaissance type weaponry, and at other

© 2020 Timothy Thomas

*Approved for Public Release. The views expressed in this document are those of the author and do not reflect the official policy or position of MITRE, the Department of Defense, or the U.S. Government.*



**Timothy L. Thomas** is an analyst for the MITRE Corporation. He worked for 27 years at the Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas. He retired from the U.S. Army as a Lieutenant Colonel in the summer of 1993. Mr. Thomas received a B.S. from West Point and an M.A. from the University of Southern California. He was a U.S. Army Foreign Area Officer who specialized in Soviet/Russian studies. His military assignments included serving as the Director of Soviet Studies at the United States Army Russian Institute (USARI) in Garmisch, Germany; as an inspector of Soviet tactical operations under CSCE; and as a Brigade S 2 and company commander in the 82nd Airborne Division. Mr. Thomas has done extensive research and publishing on military affairs about both Russia and China. He served as the assistant editor of the journal *European Security* and as an adjunct professor at the U.S. Army's Eurasian Institute, and was an adjunct lecturer at the USAF Special Operations School.

times IWes are presented more simply as weapons that help in the manipulation of social media and propaganda. The West seldom considers information to be a “weapon” as Russia does, nor does the West break the term into information-technical and information-psychological aspects.

The information-technical aspect of IWes includes technologies used extensively by Russia and many other nations in global positioning, reconnaissance, electronic warfare, and other types of equipment worldwide. The information-psychological aspect refers not only to Russia's use of information as an online weapon in the social and political arenas, which has become unsettling to Western audiences, but also to Russia's use of disinformation, fake news, non-governmental organizations, and a tendency to define objective reality as the Kremlin sees fit, and thus avoid “the truth.” Their use appears to be a modern version of Soviet active measures, which were operations developed years ago in Section A of the First Chief Directorate of the KGB. They aimed to shape operations abroad and influence events in another country and were often referred to as “political warfare.” Related terms were “assistance programs” or “assistance operations,” tactics designed to change the policy or position of a foreign government in a way that would “assist” the Soviet position. A Russian foreign intelligence officer who defected to the US in 2000 noted that there is no difference between “active measures” and “assistance operations,” and that when the KGB went away after the demise of the Soviet Union, the active measures office was renamed to assistance operations. Active measures reportedly were based on 95 percent objective information “to which something was added to turn the data into targeted information or disinformation.”<sup>[3]</sup>

Thus, Russian IWes must be considered for its utility in military, political, and psychological warfare, plus also its utility in manipulating news and social media.



As a result, IWes have become non-nuclear strategic weapons of choice. This article will examine several Russian views of IWes that cover these aspects, beginning with the bigger picture of IWes as strategic weapons. That discussion is followed by an overview of the Russian military literature that has addressed IWes over the past two decades. The discussion includes theater information weapons, information-strike weapons, cyber weapons, and social-media weapons, among others. The analysis concludes with a very brief commentary by one Russian specialist about the next generation of weapons, such as quantum computing and artificial intelligence concerns.

## THE BIG PICTURE: IWES AS NON-NUCLEAR STRATEGIC WEAPONS

IWes are considered non-nuclear strategic weapons in Russia due to their wide reach, even to continents far away (thus, a planetary weapon). According to Russian new-generation warfare expert Vladimir Slipchenko, IWes have also enabled a shift from a “quantitative-force sphere to a quantitative-intelligent sphere.”<sup>[4]</sup> He adds that countries are creating “strategic non-nuclear forces, which will find wide use in new-generation wars and subsequently also will take on a deterrence function.”<sup>[5]</sup> Numerous weapons depend on information technologies. Acoustic, electromagnetic effect, radiation, beam, and heat weaponry<sup>[6]</sup> are under development as is the “unity of intelligence collection and destruction,” namely the development of reconnaissance-strike and reconnaissance-fire complexes.<sup>[7]</sup> Slipchenko views the development of space groupings as a key shift as forces transition from a ground-based force to one based on aerospace and information. Intelligence collection from space will provide information that “will become the basis for planning massive high-precision strikes in the course of a strategic air-space-sea strike operation.”<sup>[8]</sup>

Slipchenko’s thoughts coincide with a Russian concept known as the Strategic Operations to Destroy Critically Important Targets (SODCIT) as discussed by numerous outlets. In 2010, a *Red Star* article flagged changes in the nature of wars that would manifest in the various forms in which the Armed Forces are used: “SODCIT has been developed.”<sup>[9]</sup> Retired Colonel General Viktor Barynkin added that “it has become expedient to combine strategic defensive and offensive operations and strategic operations in the ocean theater of hostilities into a single strategic operation.”<sup>[10]</sup>

In conducting such operations, the expansive reach of IWes will play a crucial role. For example, as the Russian journal *Air-Space Defense* stated in 2013:

It is possible to use various space systems in support of each of these operations. Thus, supporting a strategic operation to destroy critically important enemy targets necessitates the use of space-based means of reconnoitering these targets; electronic intelligence assets; meteorological reconnaissance assets in the interests of a proper selection of attack weapons and their combat employment methods; and space-based navigation, communications, relay, and strike evaluation systems.<sup>[11]</sup>

As noted, these assets rely on information technologies.

Thus, the term SODCIT implies the extended use of IWe as non-nuclear strategic weapons or assets. Such use in conjunction with aerospace forces or precision-guided munitions is significant since both possess long-reach capabilities into the depth of an adversary's territory anywhere on the globe. Russian planetary warfare theorists must find such concepts intoxicating. For Western analysts, SODCIT should raise concerns as to what Russia is planning.

How did Russia ultimately arrive at this conclusion that IWe provides a non-nuclear strategic capability? The following discussion that has transpired over the past two decades offers how the concept of IWe gradually evolved and incorporated new developments in information technologies, which in turn led to new ways to consider information-technical and information-psychological applications of IWe.

### **THE FIRST IMPORTANT IWE DISCUSSIONS**

Detailed descriptions of IWe and their uses began to develop slowly in the 1990s. One of the first (and still considered outstanding) Russian articles to define and discuss an IWe is the article by Major S.V. Markov, which was authored and published in 1996 in the journal *Bezопасnost (Security)*. Leading specialists still refer to his many thoughts and definitions. Markov defined an IWe as:

A specially selected piece of information capable of causing changes in the information processes of information systems (physical, biological, social, etc.) according to the intent of the entity using the weapon.<sup>[12]</sup>

This understanding of IWe and its impact on the information-technical and information-psychological activity of Russia produces a much different national will and language of dialogue than that to which the West is accustomed. Markov is convinced that international and state control over the creation and use of IWe is essential.<sup>[13]</sup>

According to Markov, IWe can be used in the following ways:

- ◆ To destroy, distort, or steal data files
- ◆ To mine or obtain the desired information from these files after penetrating defense systems/firewalls
- ◆ To limit or prevent access to them by authorized users
- ◆ To introduce disorganization or disorder into the operation of technical equipment
- ◆ To completely disable telecommunications networks and computer systems and all the advanced technology that supports the life of society and the operation of the state<sup>[14]</sup>

In 2000, the work of five authors at the Institute of Systems Analysis superseded Markov's IWe article in importance. They wrote the first authoritative, detailed introduction to, and explanation of, IWe in a pamphlet titled *The Information Weapon—A New Challenge to International*

*Security*,<sup>[15]</sup> which describes various forms of IWes. One author, Andrey Krutskikh, became President Putin's point man on cyber issues and where he continues to serve today.

These authors classified IWes based on several attributes to include single and multi-mission/universal purposes; short- and long-range operations; individual, group, and mass disruption or destruction capabilities; various types of carriers; and destructive effect. They further classified IWes as belonging to one of six forms:

1. Means to precisely locate equipment that emits rays in the electromagnetic spectrum and destroy that equipment by conventional fire
2. Means to affect components of electronic equipment
3. Means to affect the programming resource control modules
4. Means to affect the information transfer process
5. Means to disseminate propaganda and disinformation
6. Means to use psychotronic weapons

The pamphlet then discussed the significance and potential types of each of these weapons. The authors analysis of the fifth and sixth forms, which, because they are less prominently covered in the Western press, merit discussion. The fifth form, propaganda and disinformation, can change the information component of command and control (C2) systems by creating a virtual picture that alters reality, changes the system of human values, and manipulates the moral-psychological life of the enemy population. This type of weapon can create disinformation in secure systems and alter navigation systems, information and meteorological-monitoring systems, precision-time systems, and so on.

The sixth form, psychotronic weapons, describes weapons that leverage psychology and the subconscious to attack a person's will, and otherwise suppress and/or temporarily disable or zombify that person. These weapon types include:

- ◆ Psycho-pharmacological substances
- ◆ Psycho-dyspeptics
- ◆ Tranquilizers, anti-depressants, hallucinogens, and narcotics
- ◆ Specially structured medicines
- ◆ Special-beam generators that affect the human psyche
- ◆ Special video graphic and television information  
(25<sup>th</sup> frame effect, elevating blood pressure, inducing epileptic seizures, etc.)
- ◆ Means for creating virtual reality that suppresses the will and induces fear  
(e.g., projecting an image of "God" onto clouds, etc.)
- ◆ Technologies of zombification and psycholinguistic programming<sup>[16]</sup>

The authors note that information technologies can serve as IWes, which are integral components of high-precision ammunition that can be used to guide missiles via position finding and reconnaissance, as well as by visual, electronic, and other means.

### MOVING ON: INTERESTING 2001-2019 DISCUSSIONS

Russia's perception of the West's focus on noncontact warfare and advanced cyber weapons in the 1990s led Russian theorists to conclude that adversaries wanted to develop a "clean" war run by special agents and programmers against a still vulnerable Russia. This led Russian authorities to envision IWes as helping to offset the Kremlin's national security weaknesses. Russian theorists saw the many benefits of IWes and praised them for their universality, covertness, and variety of implementation forms (software and hardware), their radical effects and ability to select a precise time and place of employment, and, finally, their cost-effectiveness. But recognizing these attributes also raised concerns for Russia's national security,<sup>[17]</sup> since other nations were farther along in IWe developments.

The following discusses specific elements of Russia's focus on IWes over the past two decades and demonstrates the growing importance of the concept and how it has been integrated, through Russian eyes, into information warfare and its information-technical and information-psychological components; and how IWes have underscored the growing importance of nonmilitary means to influence and win confrontations.

In 2001, the PIR Center in Moscow published a paper that included a key chapter on IWes, noting that, like the military, information superiority now determines battle outcomes. Invariably, the first to process battlefield information is less vulnerable. Disabling an opponent's command and control systems is key to information superiority. IWes can be high-precision weapons, electronic warfare assets, electromagnetic pulse weapons, or software viruses, among others. The paper noted that an IWe's effectiveness in achieving information warfare missions is often pivotal.<sup>[18]</sup> The authors then discussed the same six IWe types and their characteristics and effects as were discussed by the 2000 IWe pamphlet authors—no surprise, because one of the 2000 pamphlet authors also coauthored the PIR Center report (V.N. Tsygichko). IWe effects were divided into three areas: information technologies (as components of munitions and reconnaissance, propaganda, and software systems), energy (as components of EW, microwave, and cruise, or unmanned aerial vehicles), or chemical (gases, aerosols, pharmacologic agents, etc.).<sup>[19]</sup> Several other IWe advantages included general freedom of access to many information systems, especially in social media; the blurring of traditional legal and ethical borders (are we witnessing a crime or an act of war?); the difficulty in controlling perceptions due to the wide range of "facts" available; and the potential for the covert preparation of a battlefield years in advance through the placement of specific software.<sup>[20]</sup>

In 2002, in an important article in *Armeyskiy Sbornik* (Army Journal) by Vladimir Slipchenko, who used the term "new-generation warfare" as early as 2000, noted that information's role

will only grow in the coming century. IWes will be system-destroying, he noted, as they will disable entire combat, economic, and social systems, rendering them an effective non-nuclear strategic weapon. Offensive means include destroying or disrupting an adversary's information infrastructure, his process of operational command and control, and attacks on computer networks. Defensive measures include operational and strategic camouflage, physical defense of information infrastructure facilities, disinformation, electronic warfare, and other means. Slipchenko added that electronic suppression would remain the most important component of a nation's information resources, predicting they eventually would become an independent countermeasure. He also flagged cybernetic warfare as a promising potential element of independent development.<sup>[21]</sup>

Also, in **2002**, two authors described IWes as nonlethal weapons (NLWs), noting the development of the mass media as an information NLW prerequisite. Of interest is that psychological NLWs also were considered as IWes but had not yet been scientifically confirmed. These NLW types included telepathy, telekinesis, clairvoyance, and other psychological means,<sup>[22]</sup> all measures under study in Russia for decades but have yet to produce known discernable results.

In **2003**, an article in the journal *Military Thought* noted that the Cold War's end brought with it a desire to eliminate many weapons of mass destruction. This caused the military to focus more attention on precision-guided and other IWes, both lethal and nonlethal. The Persian Gulf War, the article noted, integrated precision-guided weapons with global navigation, intelligence, communications, command and control, and electronic warfare systems and created theater information weapons (TIWes). Specialists began to consider information-strike operations, whereby a force could achieve military objectives without land forces. These authors viewed TIWes as the information-technical component of IWes. The information-psychological component, on the other hand, is designed to break the enemy's will to resist, where the main targets are troop morale, public opinion, and the decision-making systems of the opposing side,<sup>[23]</sup> to include using psychotropic substances or manipulative information amid distracting messages. New technologies increase the opportunities to develop and use such effects as neuro-linguistic programming.<sup>[24]</sup>

In **2007**, Sergey Ivanov, Russia's Defense Minister from 2001 until 2007, noted the important potential of IWes to influence the conduct of future wars. He was particularly impressed with the widespread applicability of IWes in conducting operations without becoming involved in a military conflict:

The development of information technology has resulted in information itself turning into a certain kind of weapon. It is a weapon that allows us to carry out would-be military actions in practically any theater of war, and most importantly, without using military power.<sup>[25]</sup>

In **2011**, two Russian military specialists wrote on information-strike operations in the journal *Armeyskii Sbornik (Army Journal)*. They viewed the classic triad of fire, strike, and maneuver as no longer capturing the essence of a battle or operation. Radio-electronic, electronic-fire, and

information-strike operations were the new forms of armed struggle. The latter is particularly important as defined below:

The information-strike operation (ISO) is the totality of mutually associated information strike engagements (*srazhenie*), information-strike battles (*boi*), and information strikes (*udar*), coordinated with respect to goal, missions, place, time, and method of conduct, carried out with the aim of disorganizing an adversary's troop and weapons command and control system and destroying his information resources.<sup>[26]</sup>

IWes conduct information strikes against an adversary's information resources. The types of strikes include information-psychological (which disinform or mislead an adversary), information-psychotropic (to disrupt a person's psyche), radio-electronic, and program-computer. ISOs help gain information initiative and superiority, including command and control of troops and the adversary's reflexive control. ISOs have no spatial limitations, a variety of forms and methods of use, no weather or seasonal constraints, can often be used covertly, and can target command posts and communication nodes.<sup>[27]</sup>

ISOs can be conducted in three stages. First, information support systems of command and control for intelligence, air defense, and rocket defense are disorganized. Second, under the cover of jamming, destructive strikes are made—operational-tactical and tactical rockets. Third, information support of tactical and army aviation and field artillery is disorganized.<sup>[28]</sup> To prepare an ISO, an adversary's command and control system must be studied and exposed, and objectives for fire and radio-electronic destruction determined in advance. Disorganizing the enemy's command and control system is critical to planning and coordinating friendly fire destruction elements.<sup>[29]</sup>

The authors then note the various types of information-psychological weapons that will enhance an ISO, and energy-information-psychological weapons under study for ways to modulate super high frequency ultrasonic infrared waves that affect the human nervous system. Psychotropic-information weapons use narcotics and chemicals to produce information-control effects on biological processes and the nervous system. Technical means (e.g., generators) of virtual information-psychological and other types of weaponry offer different potential capabilities to affect the human psyche (author's note: no actual results were offered, just these theories). Information-psychological weapons are to be integrated with fire, radio-electronic, and energy effects to broaden the operational-strategic methods for achieving ISO goals. The ISO is basically an offensive action, but it can acquire a defensive character if needed.<sup>[30]</sup>

An influential 2012 article entitled "Information Weapons: Theory and Practice of Their Employment in Information Warfare" views the infosphere as an inexhaustible information space, supply and replenishment source, and one that also features the compactness of information carriers, and bloodless responses—all infosphere features that have exponentially intensified information warfare. IWes can at least be partially kept secret, can cross borders and impact sovereignty, and can be used in both military and civilian structures. More importantly, the

authors stated that IWeS cause the greatest losses when used against command and control systems and the human mind.<sup>[31]</sup>

The authors classified IWeS according to effects, which they termed as physical, informational, software, or radio-electronic. Physical effects included specialized storage batteries for high-voltage impulses, the means to generate electromagnetic impulses, graphite bombs, and microbes that interfere with electronic circuits and insulation materials. Information effects included mass information resources, global networks, and voice “disinformation” stations. Software attack weapons included computer viruses, logic bombs, and the means to suppress information exchanges. No radio-electronic effects were offered. However, “dynamic IWeS” were defined as a “unified system of comprehensive, combined, beam, targeted, and strike employment of all forces and means of technical, communications, and information-psychological effects against the subconscious of the objective of the attack.”<sup>[32]</sup> Methods for implementing dynamic IWeS are mathematically, algorithmically, or software-hardware based, and are most effective when employed as a set in offensive, defensive, or support forms.<sup>[33]</sup> The authors noted that information-psychological effects result from:

A purposeful psychological attack against concrete areas of the human mind, the minds of a group of people, or the public consciousness as a whole. Effects can be implemented with respect to the means of information stimuli by using the entire spectrum of methods and forms of technical, visual, aural, medical, physical, painful, and virtual suppression of the will.<sup>[34]</sup>

Electromagnetic weapons (EMW) are well-known for disrupting or interfering with information system operations. They can disrupt a country’s economy, production, and defense capabilities. Disrupting systems that exchange information for command decisions can have serious consequences. C4ISR is the main target of EMW effects. It was noted that “the principle of EMW action is based on short-term electromagnetic radiation of great power, capable of incapacitating radio-electronic devices that comprise the basis of any information system.”<sup>[35]</sup>

The authors conclude as follows:

Universality, covertness, variety of the forms of software and hardware implementation, the radicalism of effects, adequate choice of time and place of employment, and, finally, cost-effectiveness make IWeS extremely dangerous. They are easily camouflaged as protection resources of, for example, intellectual property. They make it possible to even conduct offensive operations anonymously, without a declaration of war.<sup>[36]</sup>

Near the end of 2012, S.G. Chekinov and S.A. Bogdanov defined the initial period of war (IPW) in *Military Thought*, as the time when forces are deployed pre-conflict, to create favorable conditions for committing their main forces. Under the new military, political, and economic conditions, the authors attribute special significance to IPW for winning a conflict:<sup>[37]</sup>

The IPW may become the hardest phase in which the warring sides will be striving to make the most of the power of its groups of forces built up in advance and deployed in secret to achieve the main goals of the war. This period will be the most critical phase of the war and have a great effect on its outcome.<sup>[38]</sup>

Of interest are malware and other information technologies secretly placed in the infrastructure or computers of potential opponents in peacetime that would help accomplish some of the main means for winning a war, such as totally upending an opponent's command and control system. Such technologies are IWes. The authors noted that "major military, political, and strategic objectives of the war must be achieved in its initial period."<sup>[39]</sup>

In early November **2013**, the State Duma Security and Anticorruption Committee recommended amending a Federal Security Service (FSB) law to allow police investigations to counter threats to Russia's information security, such actions previously permitted only as to state, military, economic, or environmental security threats. The report indicated that harmful software, for example, can be used as an information weapon<sup>[40]</sup> that could threaten security. That same year, Russia's Security Council noted that information and communication technologies are a looming threat as IWes, since they can threaten strategic stability, violate the territorial integrity of other nations, and act in both the military and political spheres of interest.

In **2013**, Chekinov and Bogdanov discussed new-generation warfare, highlighting on numerous occasions the importance of information technologies,<sup>[41]</sup> noting that "decisive battles in new-generation wars will rage in the information environment," where computer operators will manipulate computers far away from the conflict. Information operations will induce world public opinion to accept the need to restore democracy and fight tyranny.<sup>[42]</sup> Once information superiority is achieved in peacetime; conflict may even be avoided. If a conflict appears inevitable, it is visualized information technologies will heavily influence and possibly dominate its opening phases, as there will emerge a targeted information operation, an electronic warfare operation, and high-precision weaponry loaded with information technology.<sup>[43]</sup>

In **2015**, at a presentation in Garmisch, Germany, noted Russian information warfare experts I.N. Dylevsky and S.A. Komov offered a paper titled "Rules of Conduct in Information Space—An Alternative to an Information Arms Race," noting that "[a]nother aspect of confrontation in the information sphere is a rapid advancement and proliferation of information weapons."<sup>[44]</sup> Their use can lead to industrial disasters or, worse yet, critical infrastructure (finance, energy, transport, etc.) destruction. The authors, while urging that it was time to adopt universal laws to prohibit their development,<sup>[45]</sup> did not expand on how this could be done, or how nations could control the risk of their development elsewhere.

Later that year, *Military Thought* described nonlethal weapons (NLWs) as effective information warfare assets, implying their potential as an IWe. In handling internal issues, NLWs can "defuse the bellicose moods stoked by propaganda and isolate the most outrageous advocates of the indiscriminate use of military force."<sup>[46]</sup> Ironically, the "mood" of recent anti-Kremlin



demonstrations in Moscow was provoked or exacerbated by the Kremlin's decision to keep certain people off election ballots. So, moods can either be "provoked" or "defused" (with NLW) by the same government officials.

Russia's *National Security Strategy*, published in 2015, referred 36 times to the term "information" without ever mentioning the term "cyber." The primary use of information, it seems, is as an instrument "set in motion in the struggle for influence in the international arena" (along with political and financial-economic instruments). The *Strategy* reported that confrontation in the global information arena is "caused by some countries' aspiration to utilize informational and communication technologies to achieve their geopolitical objectives, including by manipulating public awareness and falsifying history." Information is also mentioned as one way to enhance strategic deterrence. Information associated with extremism or terrorism is taken to be a significant threat to public security and, countering such threats requires an information infrastructure that ensures the public's access to information on issues relating to the sociopolitical, economic, and spiritual life of Russia's citizens.<sup>[47]</sup>

In 2016, during his annual speech at the Academy of Military Science, General Staff Chief Valery Gerasimov discussed the impact of so-called "color revolutions" and how their utility could be quickly furthered through the adaptive use of information resources as a weapon:

Essentially, any "color" revolution is a state revolution organized from without. Their basis is information technologies, which envision the manipulation of the protest potential of the population in combination with other nonmilitary means. Here, mass targeted effects on the consciousness of the citizens of a state—the objects of aggression by means of the global "Internet" network—acquire important significance. Information resources have essentially become one of the most effective types of weapons. Their extensive use makes it possible to "shake up" the situation in the country from within in a matter of days.<sup>[48]</sup>

"Information resources" the West uses against Russia, according to a *New York Times* source, are nongovernmental organizations (NGOs) and operations aimed at the young. For example, President's Putin's 2007 speech in Munich expressed concerns about NGOs, alleging they "are used as channels for funding, and those funds are provided by governments of other countries." That flow of foreign money to assist opposition political organizations in Russia, he said, is "hidden from our society. "What is democratic about this?" he asked. "This is not about democracy. This is about one country influencing another."<sup>[49]</sup>

In 2017, Chekinov and Bogdanov shifted focus from new-generation wars to the importance of "new-type" warfare. stating that globalization threatens a "new type" of war, which could "become the pivot of historical life in the 21<sup>st</sup> century."<sup>[50]</sup> New-type warfare is characterized using "political pressure, information sabotage, cashing in on humanitarian issues, secret-service activity, and unfair and cunning diplomacy."<sup>[51]</sup> Earlier in the article, the authors addressed the growing impact of information warfare. Information operations use manipulated information, computers, and telecommunications technologies to suppress adversaries by disorganizing

command and control and introducing chaos into their work. This work misinforms army personnel and the population and psychologically crushes them.<sup>[52]</sup> The realm of the virtual, both informational and cognitive, is exploited.<sup>[53]</sup> Again, while not explicitly mentioning IWes, the article clearly views IWes as major components of new-type warfare.

In 2019, the journal *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)* published an article on the impact of information processes on Russia's national security. It stated that the information society, globalized information processes, and the democratization and heightened importance of socio-political factors in society had created an information struggle. Internally, the struggle is about controlling large numbers of people. Externally, the information struggle rages both in times of peace and war among states, regardless of whether the states are allies or enemies. Twenty-first century struggles include a state's information capabilities, which work to achieve the strategic advantages<sup>[54]</sup> that come from information superiority.

Information, the authors note, moves through space and time via processes of "searching, collecting, storing, processing, presenting, accumulating, disseminating, and decision-making."<sup>[55]</sup> Depending on how information is used and where it is located (in military weapons technology, in a human mind, in command and control processes, etc.), it produces different effects (precise targeting, manipulation of data, etc.). The authors defined IWes as follows:

Information weapons are the totality of technical, software, and other special resources, constructively intended for the formation of information effects for the purpose of disrupting information processes by means of effects against the elements of an information resource (information target) by a special pattern of organized flows of emissions of energy of different physical natures or a specific pattern of selected and structured information.<sup>[56]</sup>

The authors believe the concept of "means of information effects" more broadly describes the essence of IWes. Technical effects, linguistic and software products, and other means can produce effects against an opposing side's information resources. Effects used to gain information superiority against an opponent include radio-electronic warfare resources, software that disables automated C2 systems, psychotropic generators, special pharmacological means, and the mass media. Information superiority was defined as superiority in timeliness, reliability, and completeness attained by C2 organs for use in the processing and timeliness of decision making and control in the execution of plans.<sup>[57]</sup>

A final 2019 article by a US author, discussed Russia's use of the "big lie," that is, Russia's tendency to define objective reality as the Kremlin sees fit and thereby avoid responsibility for the "truth." This is a different type of IWe. The article described Russia's recent admonition to Iran never to admit guilt in the downing of the Ukrainian airliner that it had recently caused. A deputy head of Russia's State Duma's Defense Committee noted that it was far more important to blame the US.<sup>[58]</sup> This has been a typical Russian response to avoid responsibility at all costs,

even to the detriment of its own credibility. Russia is quick to openly deny complicity in any accusation leveled against it by other nations. To date, its responsibility for the shutdown of MH-17 airliner over Ukraine and its involvement (based on credible evidence) in the poisonings of former Russian intelligence operators Aleksandr Litvinenko and Sergey Skripal (both on UK territory) are such examples. So is its failure to accept responsibility for the doping of its athletes in the Sochi Winter Olympics, a charge first levied by a Russian!

## FROM INFORMATION WEAPONRY TO KOKOSHIN'S TECHNOSPHERE

Now shifting attention from IWes to artificial intelligence (AI) and quantum computing issues, while these topics are beyond the scope of this article, their mention is important, given their significance in the continuing evolution of IWes.

Andrey Kokoshin, former Secretary of the Russian National Security Council and Deputy Defense Minister, is a renowned researcher on military and scientific issues. He wrote in a 2019 issue of the *Journal of the Academy of Military Science* that the military technosphere is a complex combination of technologies from several generations, and in several dimensions, that must be studied and used to forecast and implement change. These technologies will affect both operational and strategic plans. Various components of the technosphere, to include the combat and non-combat employment of forces and means, need to be assessed<sup>[59]</sup> for how technical issues can strengthen or weaken their use. Crucial technosphere developments currently include AI and quantum computing capabilities, along with the use of information influence.

Kokoshin stated that the ability to impose information effects on an opponent, including political and psychological effects, can deter confrontations. Each effect relies on “a persuasive, carefully thought-out demonstration of our military-technical and operational-strategic capabilities.”<sup>[60]</sup> Information confrontations can include fakes and deliberate disinformation, and these can contribute to an escalation of the situation and affect decision-makers. While never citing the term “IWes” directly, Kokoshin describes AI systems, robotics, and military confrontations in space all as information-based technologies, thus implying that they are IWes.

Kokoshin views AI's development strategy as complex, requiring consideration of uncertainty and risks: some (if not all) AI applications may have unexpected consequences, particularly when decision-making and command and control issues are at stake. Further, leaders need information as to political-military, operational-strategic, and tactical situations during information confrontations and struggles for cyberspace superiority. The last two issues must be included in war games to create a precedent for decision-making support systems.<sup>[61]</sup>

Kokoshin also views quantum technologies and quantum cryptography as critically important. Because China may have the edge with quantum telecommunications network superiority, he also believes that China can perhaps deliver “a blow against the contemporary information-centric methods of waging war” that the U.S. Armed Forces have developed.<sup>[62]</sup>

## CONCLUSIONS

Russia is far removed from the days when it threatened the US with a nuclear attack if an information attack was conducted against the Kremlin. Russia now possesses its own arsenal of IWes, one with different forms than what the West is familiar with. Russia believes IWes are non-nuclear, strategic weapons capable of inflicting numerous types of destruction or influencing potential opponents, from disorganizing command and control and disabling critical infrastructure to manipulating and persuading public opinion and causing chaos in state administrations and electoral processes. Information technologies lie at the center of IWes and, while they can be found in the arsenals of most nations, they are used in different information-technical and information-psychological ways by Russia. Information resources are used to manipulate objective reality in favor of the Russian perception of events, all the while disregarding logic and the accumulation of available evidence and proof that totally offset the Russian version of events.

Russian theorists focus their IWes in the following characteristics, types, advantages, targets, and challenges:

- ◆ IWe characteristics: universality, covertness, variety of software and hardware implementation, radicalism of effects, adequate choice of time and place of employment, and, finally, cost-effectiveness
- ◆ IWe types: NLWs, color-revolutions, NGOs, high-precision weapons, electronic warfare assets, electromagnetic pulse weapons, software viruses, energy-information-psychological weapons; psychotropic-information weapons; technical means (generators, etc.) of virtual information-psychological weaponry; and information-psychological weapons integrated with fire, radio-electronic, and energy effects
- ◆ IWe advantages: can be used in secret, can cross borders with impunity, and can be used against military and civilian structures; offer freedom of access to adversary information systems, such as social media; and allow for the covert preparation of battlefields years in advance with placement of specific software in an adversary's cyber operations
- ◆ IWe targets: warfighting, economic, and social systems, along with computers; programmable apparatuses, command and control means, communication and decision-making channels, and the human intellect and mass consciousness
- ◆ IWe problems (Note: this is a Russian perspective): IWes threaten strategic stability and the violation of territorial integrity; it is hard to get UN agreement to limit IWe development; it is important to guard against the Western use of color revolutions and nongovernmental organizations to falsify history and manipulate public opinion against Russia; we must be vigilant for information sabotage

- ◆ IWe effects: physical, informational, software, or radio-electronic; special pharmacological means and the mass media; information technologies that intensify the accuracy of munitions and reconnaissance assets and offer the pervasive application of propaganda and software; energy (as components of EW, microwave, and cruise or unmanned aerial vehicles); and chemical (gases, aerosols, pharmacologic agents, etc.)

In Summary, the Russian understanding of an IWe is much broader than how the term might be understood in the West. There is much for analysts to consider as they ponder Russian access to and use of the IWe, especially as Russia will continue to search for new and innovative applications of their use. ♥

**NOTES**

1. The "IWe" acronym is used to distinguish the term from information war and irregular war, which are both shortened to IW and cause enough confusion without adding another IW acronym.
2. V.I. Tsybal, "The Concept of Information Warfare," presentation at a September 1995 conference in Moscow, Russia, 7, attended by the author of this article.
3. Andrei Soldatov and Irina Borogan, *The New Nobility*, Public Affairs New York, 2010, 108-109.
4. V.I. Slipchenko, *Beskontaktnye Voyny (Noncontact Wars)*, Publishing House Gran-Press, 2001, 55.
5. *Ibid.*, 82. Slipchenko wrote on new-generation warfare more than a decade before Bogdanov and Chekinov did so in 2013, to great fanfare.
6. *Ibid.*, 85-88.
7. *Ibid.*, 90-91.
8. *Ibid.*, 161.
9. *Ibid.*
10. *Ibid.*
11. Vasily Y. Dolgov and Yuriy D. Podgornykh, "Space as a Theater of Military Operations: On Possible Forms and Methods of Combat Employment of Space Command Forces and Assets," *Vozdushno-Kosmicheskaya Oborona Online*, April 10, 2013.
12. S.V. Markov, "Several Approaches to the Determination of the Essence of the Information Weapon," *Bezopasnost (Security)*, No. 1-2, 1996, 53.
13. *Ibid.*
14. *Ibid.*, 56.
15. V.N. Tsygichko, D.S. Votrin, A.V. Krutskikh, G.L. Smolyan, and D.S. Chereshekin, *The Information Weapon—A New Challenge to International Security*, Institute of Systems Analysis, Moscow, 2000, 20-21. This IWe discussion is taken from Timothy Thomas, *Cyber Silhouettes*, Foreign Military Studies Office, Fort Leavenworth, KS, 2005, 168-171.
16. *Ibid.*
17. N.P. Shekhovtsov and I.E. Kuleshov, "Information Weapons: Theory and Practice of Their Employment in Information Warfare," *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, 2012, No. 1, 39.
18. Aleksandr V. Fedorov and Vitaliy N. Tsygichko, "Information Weapons as a New Means of Warfare," Chapter Three, of *Information Challenges to National and International Security*, PIR Center, Moscow 2001, 69-109.
19. *Ibid.*
20. *Ibid.*
21. Vladimir Slipchenko, "A New Form of Struggle: In the Coming Century, The Role of Information in Noncontact Wars Will Only Grow," *Armeyskiy Sbornik (Army Journal)*, No. 12 2002, 30-32.
22. Vitaliy Tsygichko and Vladimir Dyachenko, "Non-Lethal Weapons," *Yadernyy Kontrol (Nuclear Control)*, 18 September 2002, 58-67.
23. S. P. Nepobedimiy and V. F. Prokofyev, "The Intellectualization of Weapons and Weapons against Human Intelligence," *Voennaya Mysl' (Military Thought)*, No. 7 2003, 26.
24. *Ibid.*, 27.
25. Oscar Jonsson, *The Russian Understanding of War*, Georgetown University Press, 2019, 94, as quoted in Steve Blank, "Russian Information Warfare as Domestic Counterinsurgency," *American Foreign Policy Interests*, 34.
26. I.N. Chibisov and V.A. Vodkin, "The Information-Strike Operation," *Armeyskiy Sbornik (Army Journal)*, March 2011, 46.
27. *Ibid.*, 46-47.
28. *Ibid.*, 47.
29. *Ibid.*, 48.
30. *Ibid.*, 48-49.
31. Shekhovtsov and Kuleshov, 35.
32. *Ibid.*, 36.
33. *Ibid.*, 36-37.
34. *Ibid.*, 37.

NOTES

35. Ibid., 38.
36. Ibid., 39.
37. S. G. Chekinov and S. A. Bogdanov, “The Initial Period of War and its Influence on a Country’s Preparation for Future War,” *Voyennaya Mysl’ (Military Thought)*, No. 11 2012, 15-16.
38. Ibid., 19.
39. Ibid., 25.
40. Unattributed report, “A State Duma Committee Has Approved Amendments Relating to Information Security,” *RIA Novosti Online (RIA News Online)*, November 8, 2013.
41. S. G. Chekinov and S. A. Bogdanov, “On the Nature and Content of a New Generation War,” *Voyennaya Mysl’ (Military Thought)*, No. 10, 2013, 13-14.
42. Ibid., 20.
43. Ibid., 23.
44. Ninth International Forum “Partnership of State Authorities, Civil, Society, and the Business Community in Ensuring International Information Security,” April 20-23, 2015, Garmisch Germany, 36.
45. Ibid.
46. D. V. Zaitsev, V. I. Orlyansky, and D. Yu. Soskov, “Nonlethal Weapons Can Be Used to Prevent Armed Conflicts,” *Voennaya Mysl’ (Military Thought)*, No. 10 2015, 51.
47. Edict of the Russian Federation President, “On the Russian Federation’s National Security Strategy,” *President of Russia Website*, December 31, 2015. See sections 13, 21, 36, 43, and 53 of the document.
48. V.V. Gerasimov, “The Organization of the Defense of the Russian Federation under Conditions of the Enemy’s Employment of ‘Traditional’ and ‘Hybrid’ Methods of Conducting War,” *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2, 2016, 20.
49. Thom Shanker and Mark Landler, “Putin Says U.S. Is Undermining Global Stability,” *The New York Times*, 11 February 2007, downloaded 9/1/2020 at <https://www.nytimes.com/2007/02/11/world/europe/11munich.html>.
50. S. G. Chekinov and S. A. Bogdanov, “The Evolution of the Essence and Content of the Notion of ‘War’ in the 21st Century,” *Voyennaya Mysl’ (Military Thought)*, No. 1 2017, 43.
51. Ibid., 40.
52. Ibid., 37.
53. Ibid., 32.
54. V. F. Lata, V. A. Annenkov, and V. F. Moiseev, “Information Confrontation: A System of Terms and Definitions,” *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2019, 128-129.
55. Ibid., 130.
56. Ibid., 136.
57. Ibid., 136-137.
58. See Julia Davis, “Russia to Iran: Don’t Admit Guilt—Blame the U.S. Instead,” <https://www.thedailybeast.com/russia-to-iran-dont-admit-guilt-blame-the-us-instead>, accessed January 11, 2020.
59. A. A. Kokoshin, “Prospects for the Development of the Military Technosphere and the Future of Warfare and Noncombat Employment of Military Force,” *Vestnik Akademii Voennykh Nauk (Journal of the Academy of Military Science)*, No. 2 2019, 26.
60. Ibid., 27.
61. Ibid., 28.
62. Ibid., 29.









---

---


# THE CYBER DEFENSE REVIEW


CONTINUE THE CONVERSATION ONLINE

 [CyberDefenseReview.Army.mil](http://CyberDefenseReview.Army.mil)

AND THROUGH SOCIAL MEDIA

 Facebook [@ArmyCyberInstitute](https://www.facebook.com/ArmyCyberInstitute)

 LinkedIn [@LinkedInGroup](https://www.linkedin.com/company/ArmyCyberInstitute)

 Twitter [@ArmyCyberInst](https://twitter.com/ArmyCyberInst)  
[@CyberDefReview](https://twitter.com/CyberDefReview)



ARMY CYBER INSTITUTE ♦ WEST POINT



---

THE ARMY CYBER INSTITUTE IS A NATIONAL RESOURCE FOR RESEARCH, ADVICE AND EDUCATION IN THE CYBER DOMAIN, ENGAGING ARMY, GOVERNMENT, ACADEMIC AND INDUSTRIAL CYBER COMMUNITIES TO BUILD INTELLECTUAL CAPITAL AND EXPAND THE KNOWLEDGE BASE FOR THE PURPOSE OF ENABLING EFFECTIVE ARMY CYBER DEFENSE AND CYBER OPERATIONS.